Se 2/4/1989

INDUSTRIAL
SECURITY
MANUAL FOR
SAFEGUARDING
CLASSIFIED
INFORMATION

DEPARTMENT OF DEFENSE

MARCH 1989

D1.6/2:

READEX FICHE best copy available

DEFENSE INVESTIGATIVE SERVICE
1900 HALF ST. S.W.
WASHINGTON, D.C. 20324-1700

March 17, 1989

FOREWORD

This manual is issued under the directional authority of, and in accordance with, Department of Defense Directive 5220.22, "Department of Defense Industrial Security Program." It establishes uniform security practices within industrial plants, educational institutions, and all organizations and facilities used by prime contractors and subcontractors having classified information of the Department of Defense, certain other executive departments and agencies, or certain foreign governments. Users of this publication are encouraged to submit suggestions for improving the publication, through channels, to the Director, Defense Investigative Service.

DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," September 1987, is hereby canceled and superseded.

This revision is required by the demands of national security as determined by the U.S. Government. It is issued pursuant to and constitutes notice prescribed by section 1A(1) of DD Form 441, "Department of Defense Security Agreement," June 1987 and section 1A of DIS Form 1149, "Department of Defense Transportation Security Agreement," September 1986.

John F. Donnelly
JOHN F. DONNELLY
Director

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, DC 20402

SUMMARY OF CHANGES

The following is a brief description of substantial changes to the Industrial Security Manual since September 1987. These changes are marked by an asterisk in the right-hand margin of the text.

Paragraph	
1c, 3cs	Adds United States Trade Representative (USTR) as new User Agency.
1i	Adds new paragraph regarding classified access during criminal proceedings. Prohibits contractors from affording access except in accordance with the Classified Information Procedures Act (CIPA).
3k	Adds definition of CIPA.
3ab	Amends definition of CRYPTO to be consistent with the CSISM.
3ae.1	Adds definition of Defense Transportation Systems.
3aq.1	Adds definition of freight forwarder.
3aq.2	Adds definition of freight forwarder clearance.
3az.3	Adds definition of Limited Dissemination (LIMDIS).
3ba.1	Adds definition of Military Assistance Programs Address Directory.
3bc	Changes definition of an MFO to include uncleared facilities.
5g	Establishes the use of the SF 312 in lieu of the SF 189-A.
5m(1)	Deletes the prohibition of classified material retention for more than five years.
5u	Adds requirement to report personal exchanges with nationals or representatives of Designated countries. Defines "personal exchange."

SUMMARY OF CHANGES

5aa	Amended to require contractor cooperation during official inspections as well as investigations concerning the handling of classified information.
5ag	Incorporates previously approved policy regarding security inspections into ISM (see ISL 88 L-2).
5ah	Deleted. Marked "Reserved."
5am	Adds requirements for perimeter controls, i.e., inspection of personal effects to prevent unauthorized introduction or removal of classified material without proper authority.
5ao	Provides for inspection by DIS of LIMDIS protective measures which must be contractually imposed.
6a(4)(f)	Modified to include requirement to report by letter when facility is under contract to be sold to a foreign owner.
6a(19)	Requires the report to include the name of employee(s) who will serve as host(s) and their clearance status. Requires defensive security briefing to be given to personnel hosting the visit and others expected to interface with the visitors.
6b(1)	Deletes requirement to submit PCL forms with adverse information report on individuals granted a contractor CONFIDENTIAL clearance. Adds requirement for the contractor to notify UA installations, if applicable, of the favorable resolution of previously reported information. Amended to reflect the requirement for a security violation report to include the administrative actions taken against the culpable individual (see paragraph 5aj).
6b(9)	Reporting requirements amended to include any "personal exchange" with nationals or representatives

SUMMARY OF CHANGES

6b(9) (con't)	of Designated countries. Additionally, for cleared employees assigned overseas a copy of the report must be submitted to OISI.
6b(11)	Amended to read SF 312 vice SF 189-A.
6c	Deleted (2) - requirement to report information concerning employee contacts with nationals or representatives of Designated countries to the FBI. This report is now required to go to DISCO (see 6b(9)).
7e(2)	Amended to include SSN, DPOB and date of clearance of responsible individual.
10g(a) 2	Deletes immigrant aliens. Access shall be limited to U.S. citizens.
13c	Amended to require that a person "cleared by the DoD" (vice cleared "TOP SECRET") accompany the person who requires TOP SECRET access.
14a	Amended to reflect the requirement to have storage approved by the CSO.
14a(3)(d)	(1) Amended to reflect construction requirements for a steel file cabinet authorized for SECRET storage, (2) amended to reflect time limitation for use of dial-type changeable combination padlocks which do not meet the requirements of FF-P-110, (3) amended to prohibit the use of filing cabinets with bar and lock padlock (unless alarmed, etc.) for SECRET material after July 1, 1998, for facilities cleared prior to June 20, 1988.
17b	New footnote 15/ which refers to use of the STU III for transmission. Corrects ARFCOS reference to Defense Courier Service (DCS) and delineates procedures for establishing a DCS account.

SUMMARY OF CHANGES

17c(4)	Deletes requirement for prior written approval of the contracting officer. Amended to reflect that transmission must be in consonance with the telecommunications security provisions of the contract or as otherwise authorized by the contracting activity.
17f	Deletes requirement to obtain prior written approval/instructions from the contracting officer and/or CSO.
19f	Establishes requirement for contractors to develop procedures to ensure that accountable classified material is not inadvertently destroyed as classified waste.
20b	Removes restrictions on PCLs for naturalized U.S. citizens from Designated countries.
20c(1)	Deletes reference to NATO RESTRICTED information. (A PCL is no longer required for access to NATO RESTRICTED.)
20k	Deletes requirement for OODEP RFI applications to go to CSO. All OODEP PCLs will go to DISCO vice CSO.
21	Amended to reflect that storage for classified material must have approval of the CSO.
24b(1)(b)	Removes restriction on naturalized citizens from Designated countries.
24b(2) & 24b(3)	Deletes requirement to routinely submit DD Form 48-2 to DISCO. An affirmative response to item 7, however, requires a copy to DISCO for a check of the PSCF.
25	Provides for the furnishing of PSQ forms to individuals being considered for employment. Prohibits the contractor from obtaining and reviewing PSQs until the individual is employed and placed on the payroll.

SUMMARY OF CHANGES

26a	Deletes requirement for OODEP PCL applications to be sent to the CSO. All PCL applications will go to DISCO. Prohibits contractor from using PSQ information for other than its intended purpose. Requires contractor review of PSQs prior to submission to DISCO.
26c	Removes restriction on interim clearances for naturalized citizens from Designated countries.
26d(1)	(1) Eliminates exception for transfer of a PCL between collocated facilities, (2) extends the time allowed for clearance transfers and reinstatements from 12 to 24 months, (3) requires completion of DD Form 48-3 for clearance reinstatements, as well as transfers, and (4) requires reinstatement of contractor-granted CONFIDENTIAL clearances to be accomplished as a new clearance action.
26f	Deleted (2), procedures relating to a concurrent clearance for OODEPs at a parent and subsidiary. Unnecessary.
26g	Incorporates requirements into paragraph 26d. Marked "Reserved."
26h	Incorporated requirements into paragraph 26d. Renumbered remaining paragraphs.
26k	Incorporated into paragraph 27.
27	Amended to allow 24 months for all categories of civilian/military personnel.
29c(4)	Amended to reflect SF 312.
29d	Requires annotation of DD Form 48-2 when administratively terminating a contractor-granted PCL.

SUMMARY OF CHANGES

29g	Changed to require the completion of DD Form 48-3 for reinstatements of administratively terminated PCLs.
30b	Deletes MFO (ii) - redundant. "Same contractor" refers to MFO situation.
31.1e	Specifies procedures for reinstatement of LAAs issued to immigrant aliens.
35, Appendix XI	Changes "alarm system" to "Intrusion Detection System (IDS)." Establishes new requirements for IDS used to supplement or supplant guards.
37d	Amended to include furnishing visit requests via facsimile.
37d(8)	Amended to include CAGE code of the contractor and the name and address of UA to assist in expeditious processing of visit verifications.
37h(8)	Added NSA (COR) to list of U.S. Government agencies who may visit contractor facilities without having furnished advance notification of intent to visit.
86	Establishes requirements and procedures for foreign nationals issued LAAs to have access to NATO classified information. Deletes requirement for a PCL for access to NATO RESTRICTED.
88c	New subparagraph. Added new requirements for transmission of NATO RESTRICTED information.
88e	Eliminates prohibition of NATO RESTRICTED from being handcarried across international borders.
92	Requires a copy of 6b(9) reports to be submitted to OISI.
96b(1)	Changes requirement to rejustify PCLs to three years.

SUMMARY OF CHANGES

99a(7)	Allows 24 months vice 12 months for PCL application for an individual on whom a security assurance was previously provided.
108.1e	Establishes requirements for marking, recording, and storing of AIS storage media.
115c	Changes required safeguarding of cleared AIS storage media to continuous protection as described in paragraph 106e until appropriately declassified.
116b	Amended to prohibit degaussing of "high-energy" tape (coercivity of 750 oersteds or greater). Specifies that high-energy tape must be safeguarded until its physical destruction.
116c(6)(b)	Changes three cycle overwrite to 3-time overwrite.
Appendix I, para. N	Deletes sample form 189-A. Replaces with SF 312 with brief explanation of form.
Appendix I, para. T	Adds information regarding DIS Form 1150 and includes sample form.
Appendix I, para E.	Amended to reflect use of the DD Form 48-3 for reinstatements of PCLs.
Appendix IV, para. F2	Amended to specify that materials must be opaque.
Appendix IV, para. F8	Changed to include requirements for other (non-entry) doors.
Appendix VI	Incorporates 32 CFR Part 2003 (as referenced in SF 312) into appendix.
Appendix XI	New appendix specifying IDS requirements.
Appendix XVI	New appendix establishing procedures for the electronic transmission of PSQs.

Appendix XVIII	New appendix establishing guidelines for use of the Secure Telephone Units (STU IIIs).
Various paragraphs (5a, 5k, 5s, 5an, 17m, 17n, 17o, 21c, 21d, 22g, 24a(h), 24b(7), 31.2, 72a, 73 and Appendix XVII)	Adds requirements unique to freight forwarders.

GLOSSARY OF ACRONYMS AND ABBREVIATIONS COMMONLY USED IN THE DoD INDUSTRIAL SECURITY PROGRAM

ACDA	U.S. Arms Control and Disarmament Agency	
ACO	Administrative Contracting Officer	
ACSI	Assistant Chief of Staff for Intelligence, Department of Army	
AIS	Automated Information System	
AISE	Automated Information System Equipment	
APO	Army Post Office	
ASD(C)	Assistant Secretary of Defense (Comptroller)	

BI	Background Investigation	
BL	Bill of Lading	

(C)	CONFIDENTIAL	
CAB	Civil Aeronautics Board	
CAGE	Commercial and Government Entity Number (formerly FSC)	
CBL	Commercial Bill(s) of Lading	
CDSS	Canadian Department of Supply and Services	
CENTO	Central Treaty Organization	
CIPA	Classified Information Procedures Act	*
CM	Candidate Material	
CNWDI	Critical Nuclear Weapon Design Information	
COMINT	Communications Intelligence	
COMSEC	Communications Security	
CONUS	Continental United States	
COR	Central Office of Record	
COSMIC-TOP SECRET	Property of NATO and Subject to Special Security Controls	
CPU	Central Processing Unit	
CRT	Cathode Ray Tube	
CSISM	COMSEC Supplement to the Industrial Security Manual	
CSO	Cognizant Security Office	
CSS	Constant Surveillance Service	
CUSR	Central United States Registry	
CVA	Central Verifications Activity	

DFARS	Defense Federal Acquisition Regulation Supplement	*
DCAS	Defense Contract Administration Services	
DCASR	Defense Contract Administration Services Region	
DCII	Defense Central Index of Investigations	
DCS	Defense Courier Service	*
DGSC	Defense General Supply Center	
DIA	Defense Intelligence Agency	
DIS	Defense Investigative Service	
DISCO	Defense Industrial Security Clearance Office	
DISCR, OGC, OSD	Director for Industrial Security Clearance Review, Office of the General Counsel, Office of Secretary of Defense	
DISP	Defense Industrial Security Program	
DLA	Defense Logistics Agency	
DNACC	Defense National Agency Check Center	
DoD	Department of Defense	
DOE	Department of Energy (formerly ERDA)	
DOT	Department of Transportation	

DSI	Defense Security Institute (formerly the Defense Industrial Security Institute (DISI))	
DSP&P	Director for Security Plans & Programs, Office of the Deputy Under Secretary of Defense (Policy)	
DTIC	Defense Technical Information Center	
DTS	Defense Transportation System	*
DUSD(P)	Deputy Under Secretary of Defense for Policy	
EAM	Electronic Accounting Machines	
EAR	Export Administration Regulation	
EEFI	Essential Elements of Friendly Information	
ENAC	Expanded National Agency Check	
E.O.	Executive Order	
EPA	Environmental Protection Agency	
FAA	Federal Aviation Administration, Department of Transportation (formerly Federal Aviation Agency)	
FAR	Federal Acquisition Regulation	
FBI	Federal Bureau of Investigation	
FCL	Facility (Security) Clearance	
FEMA	Federal Emergency Management Agency	
FMS	Foreign Military Sales	
FOCI	Foreign Ownership, Control, or Influence	
FOUO	For Official Use Only	*
(FRD)	FORMERLY RESTRICTED DATA	
FRS	Federal Reserve System	
FSC	Federal Supply Code (see CAGE)	
FSO	Facility Security Officer/Supervisor	
FSS	Federal Supply Schedule	
GAO	General Accounting Office	
GBL	Government Bill(s) of Lading	
GFE	Government Furnished Equipment	
GFP	Government Furnished Property	
GPO	Government Printing Office	
GSA	General Services Administration	
GSOIA	General Security of Information Agreement	
HHS	Department of Health and Human Services	
HOF	Home Office Facility	
HQ	Headquarters	
ICC	Interstate Commerce Commission	
IDS	Intrusion Detection System	
IFB	Invitation for Bid	
IPO	International Pact Organization	
ISB	Industrial Security Bulletin	
ISCRO	Industrial Security Clearance Review Office	
ISL	Industrial Security Letter	
ISM	Industrial Security Manual for Safeguarding Classified Information" (DoD 5220.22-M)	
ISR	"Industrial Security Regulation" (DoD 5220.22-R)	
ITAR	"International Traffic in Arms Regulation"	

KGB	Committee on State Security (Soviet Union)	
LAA	Limited Access Authorization	
LOC	Letter of Consent, DISCO Form 560	
MAAG	Military Assistance Advisory Group	
MAP	Mutual Aid Program	
MAPAD	Military Assistance Programs Address Directory	*
MDAP	Mutual Defense Assistance Program	
MFO	Multiple Facility Organization	
MIL-STD	Military Standard (Book Form)	
MTMC	Military Traffic Management Command (formerly MTMTS)	
N/A	Not Applicable	
NAC	National Agency Check	
NASA	National Aeronautics and Space Administration	
NATO	North Atlantic Treaty Organization	
NCSC	National Communications Security Committee	
NISC	Naval Investigative Service Command	
NPLO	NATO Production Logistics Organization	
NRC	Nuclear Regulatory Commission	
NSA	National Security Agency	
NSF	National Science Foundation	
OADR	Originating Agency's Determination Required	*
OASD(PA)	Office of the Assistant Secretary of Defense (Public Affairs)	
OISI	Office of Industrial Security, International	
OODEPs	Owners, Officers, Directors, Partners, Regents, Trustees, or Executive Personnel	
OPM	Office of Personnel Management	
OPSEC	Operations Security	
OSD	Office of Secretary of Defense	
OSI	Office of Special Investigations, USAF	
PCL	Personnel (Security) Clearance	
PCO	Procuring Contracting Officer	
PIC	Personnel Investigations Center	
PMF	Principal Management Facility	
PRP	Personnel Reliability Program	
PSCF	Personnel Security Clearance Files (Industrial)	
PSQ	Personnel Security Questionnaire	
PSS	Protective Security Service	
(RD)	RESTRICTED DATA	
RFI	Representative of a Foreign Interest	
RFP	Request for Proposal	
RFQ	Request for Quote	
(S)	SECRET	
SBA	Small Business Administration	
SCI	Sensitive Compartmented Information	*
SEATO	Southeast Asia Treaty Organization	
SEC	Securities and Exchange Commission	
SIOP	Single Integrated Operational Plan	
SPP	Standard Practice Procedure(s)	
SSO	System Security Officer	

TO	Transportation Officer
TPS	Transportation Protection Service
(TS)	TOP SECRET
TSEC	U.S. Telecommunications Security
TWX	Teletype Communications
(U)	UNCLASSIFIED
UA	User Agency
U.K.	United Kingdom
UL	Underwriters' Laboratories
U.S.	United States of America
USAFSS	U.S. Air Force Security Service
U.S.C	United States Code
USIA	United States Information Agency
USTR	United States Trade Representative *

TABLE OF CONTENTS

Paragraph — Page

Foreword . . . i

Summary of Changes . . . iii

Glossary of Acronyms and Abbreviations Used in the DoD Industrial Security Program . . . xi

Section I. GENERAL

1 Scope . . . 1
2 Applicable Federal Statutes, Executive Orders, and Regulations . . . 2
3 Definitions . . . 3
4 Designation of Cognizant Security Office . . . 17
5 General Requirements . . . 17
6 Reports . . . 36
7 Loss, Compromise, or Suspected Compromise of Classified Information . . . 43
8 Badges and Identification Cards . . . 44
9 DoD Sponsorship of Meetings . . . 45

Section II. HANDLING OF CLASSIFIED INFORMATION

10 Classification . . . 51
11 Marking . . . 54
12 Record of Classified Material . . . 65
13 Special Requirements for TOP SECRET . . . 68
14 Storage . . . 70
15 Alternate Storage Locations . . . 75
16 Safeguards During Use . . . 76
17 Transmission . . . 76
18 Reproduction . . . 89
19 Destruction . . . 90

Section III. SECURITY CLEARANCES

20 General . . . 95
20.1 Emergency Higher Level Access . . . 98
21 Facility Security Clearances . . . 100
22 Personnel Clearances Required in Connection with Facility Clearances . . . 102
23 Security Clearance of Negotiators . . . 106
24 Security Clearance of Additional Personnel . . . 106
25 Preemployment Clearance Application . . . 109
26 Application for Personnel Security Clearance . . . 109
27 Conversion of Clearances of Present and Former Civilian and Military Personnel of the DoD and Other Government Agencies to Industrial Clearances . . . 115

28 Contractor's Clearance Record 116
29 Administrative Termination of Personnel Security Clearances 116
30 Administrative Downgrading of Personnel Security Clearances 118
31 Access to Classified Information by Non-United States Citizens. . . . 118
31.1 Immigrant Aliens. 118
31.2 Foreign Nationals 120
31.3 Access Limitations for Immigrant Aliens, Foreign Nationals, and Firms Granted a Reciprocal Facility Security Clearance. 120

Section IV. CONTROL OF AREAS

32 Purpose 123
33 General 123
34 Area Controls 124
35 Supplemental or Supplanting Intrusion Detection Systems (IDS) 126
36 Supplanting Access Control System Devices. 128

Section V. VISITOR CONTROL PROCEDURES

Part 1. Visits to User Agency Contractors

37 General 133
38 Identification and Control of Visitors. 135
39 Visitor Record 136
40 Long-Term Visitors. 136
41 Visitor Categories and Procedures 137
42 Visits Involving Access to RESTRICTED DATA. 141

Part 2. Visits to User Agency Activities

43 General Rules -- In Addition to Paragraph 37. 142
44 Visits to User Agency Activities in the United States 142
45 Visits to User Agency Activities Outside the United States. 143

Part 3. Visits to Government Activities Other Than User Agencies

46 Visits to DOE Installations or DOE Contractors. 144
47 Visits to Activities Other Than DOE 144

Part 4. Visits to Foreign Governments and Activities

48 General 144
49 Processing Time 146
50 Use of OISI 146

Part 5. Visits in Connection With Bilateral Industrial Security Agreements and NATO Visits Procedures

51 Visits in Connection with Bilateral Industrial Security Agreements. . 146
52 NATO Visit Procedures 147

53 NATO Production Logistics Organization (NPLO) Programs Clearance and Visit Procedures 148
54 Records of NATO Visits. 148
55 Certificate of Security Clearance 149

Section VI. SUBCONTRACTORS, VENDORS, AND SUPPLIERS

56 Application to Subcontractors 151
57 Application to Sub-Subcontractors 151
58 Determination of Clearance Status 151
59 Safeguarding Ability. 152
60 Classification Guidance 153
61 Required Distribution 156
62 Notification of Selection 157
63 Unsatisfactory Security Conditions. 157
64 Disposition of Classified Information 157
65 Subcontracting With Foreign Industry. 158
66 Subcontracts Arising From Foreign Classified Contracts. 159

Section VII. CONSULTANTS

67 General 161
68 Consultant -- Type A 161
69 Consultant -- Type B. 162
70 Consultant -- Type C. 162
71 Consultants to User Agencies Employed Under Civil Service Procedures. 163

Section VIII. PARENT-SUBSIDIARY AND MULTIPLE FACILITY ORGANIZATIONS

72 Parent-Subsidiary Relationships 165
73 Multiple Facility Organizations (MFO) 166
74 Temporary Help Suppliers. 168

Section IX. SENSITIVE COMPARTMENTED INFORMATION AND COMSEC INFORMATION

75 SENSITIVE COMPARTMENTED INFORMATION 171
76 COMSEC Information. 171

Section X. GRAPHIC ARTS

77 Special Requirements for Graphic Arts 173
78 Production Control Records. 173
79 Area Controls -- Additional Requirements. 173
80 Special Conditions. 174
81 Destruction -- Special Requirements 175
82 Mailing Lists 176

Section XI. NATO INFORMATION

83 Application . . . 177
84 Authority . . . 177
85 Supervision and Orientation Requirements . . . 177
86 Security Clearances . . . 178
87 Reproduction, Preparation, and Marking . . . 179
88 Transmission of NATO Material . . . 179
89 Functions of the Contracting Officer . . . 182
90 NATO Reporting Requirements . . . 182
91 Subcontracting . . . 182

Section XII. OVERSEAS OPERATIONS

Part 1. Access to U.S. Classified Information

92 General . . . 183
93 Access to Classified Information . . . 183
94 Safeguarding U.S. Classified Information . . . 184
95 Overseas Assistance . . . 185
96 Notification of Overseas Assignment . . . 186
97 Security Briefings and Certificates . . . 187

Part 2. Access to Classified Information of Foreign Governments and International Pact Organizations Under a Security Assurance

98 General . . . 188
99 Security Assurance . . . 189

Section XIII. SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS

Part 1. General

100 Reserved . . . 191
101 Applicability . . . 191
102 Objectives . . . 191

Part 2. Requirements

103 General . . . 192
104 AIS Security Modes of Operation . . . 193
104.1 Concurrent Processing of Multiple Classification Levels . . . 196
105 Personnel Security . . . 196
106 Physical Security . . . 198
107 Reserved . . . 200
108 Reserved . . . 200
108.1 Protection of Software and Data . . . 200
109 Transmission Controls . . . 202
110 Subcontracting Controls . . . 202
111 Audit Trails . . . 203

Part 3. Procedures

112 AIS Security Approval 204
113 AIS Security Level Upgrading. 206
114 AIS Security Level Downgrading. 208
115 Media and Equipment Clearance 208
116 Media and Equipment Declassification. 209

Section XIV. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

117 Policy. 213
118 Access Requirement. 213
119 Briefings. 213
120 Records 213
121 Marking 213
122 Subcontracting and Consultants. 214
123 Transmission Outside the Facility 214

Section XV. OPERATIONS SECURITY (OPSEC)

124 Purpose 215
125 General 215
126 Applicability 215
127 Procedures for Self-Inspecting OPSEC Programs 216

Appendix I. INDUSTRIAL SECURITY FORMS

A. Application 217
B. Special Privacy Section Instructions. 217
C. "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" (DD Form 48). 217
D. "Application and Authorization for Access to Confidential Information (Industrial)" (DD Form 48-2) 221
E. "Department of Defense Personnel Security Questionnaire (Updating)" (DD Form 48-3) 224
F. "Department of Defense Personnel Security Questionnaire (Industrial)" (DD Form 49) 227
G. "Department of Defense Contract Security Classification Specification" (DD Form 254) 233
H. "Applicant Fingerprint Card" (FD Form 258). 242
I. "Request for Visit or Access Approval" (DOE F 5631.20). 245
J. "Letter of Notification of Facility Security Clearance" (DIS FL 381-R) 246
K. Reserved. 247
L. "Department of Defense Security Agreement" (DD Form 441) and "Appendage" (DD Form 441-1). 247
M. "Certificate Pertaining to Foreign Interests" (DD Form 441s). 251
N. "Classified Information Nondisclosure Agreement, Standard Form (SF) 312. 255
O. "Letter of Consent" (DISCO Form 560). 258
P. Reserved. 259

Q. "Personnel Security Clearance Change Notification" (DISCO Form 562). 259
R. Reserved. 262
S. Reserved. 262
T. "Department of Defense Transportation Security Agreement" (DIS Form 1149) and "Appendage to Department of Defense Transportation Security Agreement" 262
U. "Facility Clearance Register" (DD Form 1541) and "Registration for Scientific and Technical Information Services" (DD Form 1540) 267
V. Letter Agreement to Safeguard Classified Information for an Employee Performing Consultant Services ("Type C" Consultant). 271

Appendix II. DERIVATIVE CLASSIFICATION INFORMATION AND PROCEDURES

A. Scope and Application 273
B. Downgrading/Declassification and "Classified by" Line Procedures 276
C. Applying Derivative Markings to New Material. 277
D. Most Restrictive Marking Determination. 277
E. Downgrading/Declassification Actions for Pre-August 1, 1982 Material 278
F. Extracts of Information 278
G. Changing Classification Markings. 278
H. Release of Declassified Information 278

Appendix III. FOREIGN CLASSIFIED CONTRACTS

Table Outlining Responsibilities for Security Actions 279

Appendix IV. REQUIREMENTS FOR THE CONSTRUCTION OF STORAGE VAULTS AND STRONGROOMS

A. Application 281
B. Class A Vault 281
C. Class B Vault 282
D. Class C Vault 282
E. Structural Design 283
F. Strongrooms 283
G. Approvals 284

Appendix V. REQUIREMENTS FOR THE CONSTRUCTION OF CLOSED AREAS

A. Application 285
B. Requirements. 285

Appendix VI. EXTRACTS OF THE ESPIONAGE AND SABOTAGE ACTS, OTHER FEDERAL CRIMINAL STATUTES, AND EXECUTIVE ORDER 12356, AND 32 CFR PART 2003 287

Appendix VII. GUIDANCE FOR PREPARATION OF SECURITY BRIEFINGS

A. Defense Security Briefings. 317
B. Counterintelligence Awareness Briefings 319

Appendix VIII. INFORMATION REGARDING COGNIZANT SECURITY OFFICES, DISCO, DSI, AND OISI. 325

Appendix IX. USE OF ESCORTS FOR CLASSIFIED SHIPMENTS (also applies to carrier custodians)

A. General 335
B. Instructions and Operating Procedures 335
C. Functions of an Escort. 335

Appendix X. REQUIREMENTS APPLICABLE TO THE HAND-CARRYING OF CLASSIFIED MATERIAL ABOARD COMMERCIAL PASSENGER AIRCRAFT

A. General 337
B. Background. 337
C. Routine Processing. 337
D. Approval. 337
E. Authorization Letter and Identification Card 338
F. Preparation for Transmission. 339
G. Special Processing. 339
H. Incident Situations 340
I. Briefing. 341

Appendix XI. INTRUSION DETECTION SYSTEM (IDS) REQUIREMENTS

A. Purpose 343
B. IDS Approval. 343
C. IDS Equipment 343
D. IDS Installation. 343
E. Certification of Compliance 343

Appendix XII. DOCUMENTS ACCEPTABLE FOR PROOF OF U.S. CITIZENSHIP. 345

Appendix XIII. GUIDANCE FOR CONTRACTOR SELF-INSPECTIONS

A. Facility Clearance. 347
B. Access Authorizations 347
C. Security Education. 348
D. Standard Practice Procedures. 349
E. Subcontracting. 349
F. Visit Control 349
G. Classification. 350
H. Employee Identification 351
I. Foreign Contacts/Travel 351
J. Public Release. 351
K. Classified Storage. 352
L. Markings. 352
M. Transmissions 353
N. Classified Material Controls. 354
O. Controlled Areas 355
P. Disposition 356
Q. Reproduction. 356
R. Classified Meeting. 357
S. Consultants 358
T. AIS 358
U. COMSEC/CRYPTO 359
V. International Operations. 360

Appendix XIV. EQUIVALENT FOREIGN AND INTERNATIONAL PACT ORGANIZATION SECURITY CLASSIFICATIONS. 365

Appendix XV. AREAS COVERED BY MTMC AND HOTLINE NUMBERS TO BE USED FOR EMERGENCIES 371

Appendix XVI. PERSONNEL SECURITY QUESTIONNAIRE (PSQ) ELECTRONIC TRANSMISSION PROGRAM

A. General 373
B. Background. 373
C. General Requirements. 374

Appendix XVII. TRANSPORTATION PLAN/TRANSMISSION INSTRUCTIONS 377

Appendix XVIII. SPECIAL CONSIDERATIONS FOR STU-III TYPE I SECURE TELEPHONE UNITS AT CONTRACTOR FACILITIES

A. General 379
B. Background. 379
C. Types and Models of Equipment 380
D. General Requirements. 380

Appendix XIX. INDEX 385

Section I. GENERAL

1. Scope.

a. This manual establishes the requirements for safeguarding all classified information to which contractors and their subcontractors, vendors, or suppliers have access or possession. The manual is written in terms of the most common situation where the contractor has access to, or possession of, classified information in connection with the performance of a classified contract. However, it also is applicable to the safeguarding of classified information in connection with all aspects of precontract activity including preparation of bids and proposals, precontract negotiations, and all aspects of postcontract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract, such as government-sponsored independent research and development advance agreements or User Agency (UA) programs participated in by a firm, organization, or individual on a voluntary or grant basis. Examples of the latter programs are the long-range scientific and technical planning programs and programs designed to provide planning briefings for industry. In such situations the official of the UA (or his or her designated representative) who releases or discloses the classified information to the contractor shall fulfill the responsibilities which this manual assigns to the contracting officer (such as furnishing necessary classification guidance, authorizing retention of classified material, and certifying contractors' need to attend classified meetings). In addition, as a general rule, terms such as "cleared employees," "authorized personnel," and "employees in-process for clearance," used herein, encompass all contractor employees granted a personnel security clearance or limited access authorization and those employees under consideration for access to classified information by the DoD.

b. The requirements of this manual reflect the provisions of applicable federal statutes, E.O.'s, and DoD directives.

c. The Secretary of Defense is authorized to act in behalf of the departments and agencies listed below in rendering industrial security services. This authority is contained in an exchange of letters between the Secretary of Defense and: (i) the Administrator, National Aeronautics and Space Administration; (ii) the Secretary of Commerce; (iii) the Administrator, General Services Administration (GSA); (iv) the Secretary of State; (v) the Administrator, Small Business Administration (SBA); (vi) the Director, National Science Foundation (NSF); (vii) the Secretary of the Treasury; (viii) the Secretary of Transportation; (ix) the Secretary of the Interior; (x) the Secretary of Agriculture; (xi) the Director, United States Information Agency (USIA); (xii) the Secretary of Labor; (xiii) the Administrator, Environmental Protection Agency (EPA); (xiv) the Attorney General, Department of Justice; (xv) the Director, U.S. Arms Control and Disarmament Agency (ACDA); (xvi) the Director, Federal Emergency Management Agency (FEMA); (xvii) the Chairman, Board of Governors, Federal Reserve System (FRS); (xviii) the Comptroller General of the United States, General Accounting Office (GAO); and (xix) the United States Trade Representative (USTR). *

d. The Deputy Under Secretary of Defense for Policy (DUSD(P)), his or her designee, or higher authority provides overall policy guidance for the DoD Industrial Security Program. The Director, DIS is responsible for the administration of the DoD Industrial Security Program on behalf of all UA's. Except for certain functions performed by the Commander or Head of a UA installation, with respect to those facilities or contractor activities located on the installation, the Directors of Industrial Security shall perform Cognizant Security Office (CSO) functions prescribed in this manual, with respect to all contractor facilities within their respective regions (see appendix VIII for geographical areas of responsibility).

e. UA's have the authority of, and exercise the functions of, a contracting officer as prescribed in this manual and the ISR. Certain of these functions, under delegation, are performed by the ACO.

f. This manual also shall apply to the safeguarding of foreign classified information, which has been furnished to U.S. contractors and which the U.S. Government is obligated to protect in the interest of national defense. When foreign classified information is made available to a contractor by a UA in connection with a U.S. classified contract, procedures applicable to U.S. classified information shall apply. However, when foreign classified information is made available to U.S. contractors in connection with a foreign classified contract, the responsibility for the actions, which this manual charges to the contracting officer and the contracting UA, shall be as prescribed in appendix III. Responsibilities not specifically assigned in appendix III are reserved to the foreign government agency or foreign contracting activity concerned.

g. Revisions to this manual that have been approved by the DUSD(P) will be effective the date of the change.

h. Although not a component of the Defense Industrial Security Program (DISP), the DoD Operations Security Program (OPSEC) is discussed in Section XV of this manual in order to provide contractors participating in the DISP with advice and guidance concerning OPSEC in the event they become involved with this program via UA imposed OPSEC contractual requirements. The DoD OPSEC program is applicable only to defense contractors participating in the DISP when the contractor UA determines that OPSEC measures are essential to protect classified information for specific classified contracts.

i. The provisions of this manual do not apply to proceedings in *
criminal cases involving classified information, and appeals therefrom, *
before the United States District Courts, the Courts of Appeal, and the *
Supreme Court. Contractors and their employees are not authorized to afford *
defendants, or persons acting for the defendant, regardless of their *
individual clearance status, access to classified information except as *
otherwise authorized by a protective order issued pursuant to the Classified *
Information Procedures Act (CIPA) (Public Law 96 - 456, 94 STAT. 2025) *

2. Applicable Federal Statutes, Executive Orders, and Regulations.

a. Espionage Acts, 18 U.S.C. §§ 793-799

b. Sabotage Acts, 18 U.S.C. §§ 2151-2157

c. Conspiracy Statute 18 U.S.C. §§ 371

d. Internal Security Act (1950) (in part), 50 U.S.C. §§ 781-798

e. National Security Act of 1947, as amended

f. Armed Services Procurement Act of 1947, as amended

g. Atomic Energy Act (1954), Public Law 703, 83rd Congress, as amended

h. E.O. 10104, February 1, 1950

i. E.O. 12356, April 2, 1982

j. National Aeronautics and Space Act of 1958, as amended

k. E.O. 10865, February 20, 1960

l. Federal Aviation Act of 1958, as amended

m. E.O. 10909, January 17, 1961

n. International Traffic in Arms Regulation (ITAR), Code of Federal Regulations, Title 22, Chapter 1, Parts 121-127

o. Export Administration Act of 1979

p. Mutual Security Act of 1954, as amended

q. Information Security Oversight Office (ISOO) Directive No. 1, June 23, 1982, as amended, concerning national security information

3. Definitions. The following definitions are established for the purpose of this manual.

a. Access, Accessibility. This refers to the ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures which are in force do not prevent him or her from gaining knowledge of the classified information 1/.

b. Automated Information System (AIS). An assembly of computer hardware, software and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material (see definition of Computer Hardware).

1/ The entry into a controlled area, per se, will not constitute access to classified information, if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a personnel security clearance (PCL).

c. AIS Security. The totality of security safeguards needed to provide an acceptable level of protection for an AIS and the classified data processed. Includes all hardware/software functions, characteristics and mechanisms; operational, accountability and access control procedures at the computer and remote terminal facilities; and management constraints, physical structures and devices needed to provide an acceptable level of protection for classified information in any state of storage, processing, display or communication within the AIS.

d. Alien. An alien is any person who is not a citizen or national of the U.S. (see "Immigrant Alien," paragraph 3av).

d.1. Application Software. Computer programs developed for specific functional uses and to solve particular problems, for example, navigation, fire control and flight simulation. Contrast with System Software.

e. Authorized Persons. Authorized persons are those persons who have a need-to-know for the classified information involved and have been cleared for the receipt of such information (see paragraph 3bg). Responsibility for determining whether individuals' duties require that they possess, or have access to, any classified information and whether they are authorized to receive it rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipients.

f. Candidate Material. This is material that is referred to collectively as special nuclear materials and nuclear weapons.

f.1. Carve-Out. A classified contract issued in connection with an approved Special Access Program in which the DIS has been relieved of inspection responsibility in whole or in part.

g. Classification Authority. This refers to the authority that is vested in an official of a UA to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

h. Classification Guide. This is a document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis. (Classification guides are provided to contractors by the DD Form 254, "Department of Defense Contract Security Classification Specification.")

i. Classified Contract. A classified contract is any contract that requires or will require access to classified information by the contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.)

j. Classified Information. This is information or material that is: (i) owned by, produced by or for, or under the control of the U.S. Government; (ii) determined under E.O. 12356 or prior orders to require protection against unauthorized disclosure; and (iii) so designated.

k. Classified Information Procedures Act. A law passed by Congress that provides a mechanism for the courts to determine what classified information the defense counsel can access during criminal proceedings. * * *

l. Classifier. A classifier is an individual who makes a classification determination and applies a security classification to information or material. A classifier may be a classification authority or may derivatively assign a security classification based on a properly classified source or a classification guide. Within this context, contractors may apply security classification markings based on classified source material or a DD Form 254, as required by this manual.

m. Closed Area. A closed area is a controlled area that is established to safeguard classified material, which, because of its size or nature, cannot be adequately protected by the safeguards prescribed in paragraph 16 or stored during nonworking hours in accordance with paragraph 14 (see section IV).

n. Closed Vehicle. A closed vehicle is a conveyance which is fully enclosed by sides, permanent top, and door.

o. Critical Nuclear Weapons Design Information (CNWDI). CNWDI is TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and totally contained quantities of fissionable, and high-explosive materials by type. Among these excluded items are the components which DoD personnel, including contractor personnel, set, maintain, operate, test, or replace.

p. Cognizant Security Office (CSO). The term refers to the office of the DIS Director of Industrial Security who has industrial security jurisdiction over the geographical area in which a facility is located.

q. Colleges and Universities. This refers to all educational institutions that award academic degrees, and related research activities directly associated with a college or university through organization or by articles of incorporation.

r. Communications Intelligence (COMINT). This is technical and intelligence information derived from foreign communications by other than the intended recipient.

s. Communications Security (COMSEC). COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use national security information and also includes the application of physical security measures to COMSEC information or materials.

t. Complex. A complex is a facility, or any element thereof, which consists of one or more buildings or structures physically enclosed within a common perimeter barrier that is supplemented by protective measures to inhibit unauthorized access and control authorized access.

u. Compromise. A compromise is the disclosure of classified information to persons not authorized access thereto.

u.1 Compromising Emanations. This refers to unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information (classified information) transmitted, received, handled or otherwise processed by any information-processing equipment (see "TEMPEST").

u.2 Computer Facility. One or more AIS's located within a single area.

u.3 Computer Hardware. Any physical equipment or device used in the configuration and operation of an AIS. Includes general and special purpose digital, analog and hybrid computers which perform logical, arithmetic or storage functions; and all components directly related to or operating in conjunction with such computers which are used to create, compose, collect, store, edit, process, communicate, display or disseminate information.

v. CONFIDENTIAL. "CONFIDENTIAL" is the designation that shall be applied to information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security. Examples of "damage" include the compromise of information that indicates strength of ground, air, and naval forces in the U.S. and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and revelation of performance characteristics, test data, design, and production data on munitions of war.

w. Consignee. The consignee is a person, firm, or government activity named as the receiver of a shipment; one to whom a shipment is consigned.

x. Consignor. The consignor is a person, firm, or government activity by whom articles are shipped. The consignor is usually the shipper.

x.1 Constant Surveillance Service (CSS). A transportation protective service provided by a commercial carrier qualified by MTMC to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative, however, an FCL for the carrier is not required. In addition, the carrier providing the service must maintain a signature and tally record for the shipment (see paragraph 3cg).

y. Continental Limits of the United States (CONUS). This refers to U.S. Territory, including the adjacent territorial waters located within the North American continent between Canada and Mexico.

z. Contracting Officer. A contracting officer is any government official who, in accordance with departmental or agency procedures, is currently designated as a contracting officer with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority. For purposes of this manual, the term contracting officer refers to the contracting officer at the purchasing office who is identified as the PCO and the contracting officer at a contract administration office who is identified as the ACO. Normally, the responsibilities which this manual assigns to the contracting officer during the precontract, contract award, and postcontract stages of a classified procurement will be performed by the PCO, with the ACO performing those responsibilities which arise during the performance stages of a classified contract.

aa. Contractor. A contractor is any industrial, educational, commercial, or other entity that has executed a DD Form 441, "Department of Defense Security Agreement," with a DoD agency for the purpose of performing on a classified contract or other classified procurement. The term contractor also refers to an individual who manages such an entity.

ab. CRYPTO. "CRYPTO" is a marking or a designator identifying all COMSEC keying material that is used to secure or authenticate telecommunications carrying classified, or sensitive but unclassified, government or government derived information, the loss of which could adversely affect the national security interest. (This CRYPTO marking also identifies COMSEC equipment and/or computer software containing operational keying variables.) * * * * * *

ac. Custodian. A custodian is an individual who has possession of, or is otherwise charged with, the responsibility for safeguarding or accounting for classified information.

ad. Declassification. This is the determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation.

ae. Declassification Event. This is an event that eliminates the need for continued classification of information.

ae.1 Defense Transportation Systems (DTS). Consists of Military controlled terminal facilities, Military Airlift Command (MAC) controlled aircraft, Military Sealift Command (MSC) controlled or arranged sealift and Government controlled air or land transportation. * * *

af. Department of Defense. DoD refers to the Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities).

ag. Derivative Classification. This is a determination that information is in substance the same as information currently classified and application of the same classification markings.

ag.1 Designated Countries. Those countries whose policies are inimical to U.S. interest: Afghanistan, Albania, Angola, Bulgaria, Cuba, Czechoslovakia, Ethiopia, German Democratic Republic (GDR) (East Germany including the Soviet Sector of Berlin), Hungary, Iran, Iraq, Kampuchea (formerly Cambodia), Laos, Libya, Mongolian People's Republic (Outer Mongolia), Nicaragua, North Korea, People's Republic of China (including Tibet), Poland, Rumania, South Yemen, Syria, Union of Soviet Socialist Republics (USSR) (includes Estonia, Latvia, Lithuania, and all other constituent republics, Kurile Islands and South Sakhalin (Karafuto)), Vietnam, and Yugoslavia.

ah. Document. A document is any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, engravings, sketches, working notes, and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

ai. Downgrade. This is a determination that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such a lower degree of protection.

ai.1 Essential Elements of Friendly Information. Key questions, or critical information secrets about United States intentions, military capabilities, plans or programs needed by an adversary to relate with other available information and intelligence in order to assist that adversary in reaching a logical decision. DoD military components refer to the Essential Elements of Friendly Information as EEFI. These EEFI may be disclosed through OPSEC indicators.

aj. Executive Personnel. Executive personnel are those individuals in managerial positions, other than owners, officers, or directors, who administer the operations of the facility. (This category includes such designations as general manager, plant manager, plant superintendent, or similar designations, and facility security supervisor (FSO).)

ak. Facility. A facility is a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined above.) For purposes of industrial security, the term does not include UA installations.

al. Facility (Security) Clearance (FCL). This is an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

am. Firmware. A method of organizing control of an AIS in a microprogrammed structure in addition to, or rather than, software or hardware. Microprograms are composed of microinstructions, normally resident in read-only memory (ROM), to directly control the sequencing of computer circuits at the detailed level of the single machine instruction.

an. Foreign Government Information. This is information that is: (1) provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or (ii) produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

ao. Foreign Interest. The term refers to any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the U.S. or its possessions; and any form of business enterprise organized or incorporated under the laws of the U.S., a state, or other jurisdiction of the U.S. that is owned or controlled by a foreign government, firm, corporation, or person. Included in this definition is any person who is not a citizen or national of the U.S. (An immigrant alien as defined in paragraph 3av is excluded from the definition of a foreign interest.)

ap. Foreign Nationals. This refers to all persons who are not U.S. citizens, U.S. nationals, or immigrant aliens to the U.S.

aq. FORMERLY RESTRICTED DATA (FRD). This is information removed from the RESTRICTED DATA category upon a joint determination by the DOE (or antecedent agencies) and the DoD that such information relates primarily to the military utilization of atomic weapons, and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as RESTRICTED DATA.

aq.1 Freight Forwarder. A freight forwarder is a U.S. or foreign-owned *
private firm granted authority to serve as a contractual agent to receive, *
consolidate, and store material within the U.S. and arrange for its onward *
movement to a foreign/purchasing country. An approved freight forwarder does *
not normally serve as a final destination carrier (i.e., rail, air, truck or *
ship company). Freight forwarders vary considerably in size, service, and *
capability. Most purchasing country staffs in the U.S. do not have the *
capability to effect in-country delivery of material. The freight forwarder *
undertakes these responsibilities as an agent for the customer and its *
function is an essential and integral element of the transportation cycle. *
Cleared freight forwarders are listed in the Military Assistance Programs *
Address Directory (MAPAD). *

aq.2 Freight Forwarder Clearance. A facility security clearance (FCL) *
issued to freight forwarders. Only freight forwarders that have been *
granted an appropriate FCL by the Defense Investigative Service (DIS) are *
eligible to receive, process, store or transmit U.S. classified material to *
a foreign government. A clearance of a foreign-owned freight forwarder firm *
will be limited to the country from which the ownership stems. A clearance *
of a U.S.-owned freight forwarder has no country limitations, but the using *
foreign government must designate such freight forwarder as its agent for *
classified freight. *

ar. Graphic Arts. This refers to facilities and individuals engaged in performing consultation, service, or the production of any component or end product which contributes to, or results in, the reproduction of classified information. Regardless of trade names of specialized processes, it includes writing, illustrating, advertising services, copy preparation, all methods of printing, finishing services, duplicating, photocopying, and film processing activities.

as. Hardened Container. A hardened container is a container of such strength and durability as to provide security protection to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container while in transit. Some examples of hardened containers are banded or wired boxes, wooden boxes, and closed cargo transporters.

at. Home Office Facility (HOF). The HOF is the headquarters facility of a multiple facility organization (see paragraph bc below).

au. Immigrant Alien. An immigrant alien is any person who is lawfully admitted into the U.S. under an immigration visa for permanent residence (see paragraph 31.1 for special prerequisites for clearance of immigrant aliens).

av. Industrial Security. This refers to that portion of internal security which is concerned with the protection of classified information in the hands of U.S. industry.

aw. Information. Information is knowledge that can be communicated by any means.

ax. Information Processing Equipment. Any equipment or device which electro-mechanically or electronically processes, reproduces, converts, or otherwise manipulates any form of information. The following equipment is typical: electric typewriters, reproduction copiers, word processors, composing and editing equipment, video displays, automated data processors, telecommunications equipment and systems. including teletype, facsimile and cryptographic equipment, and all interfaces, power sources, and interconnecting paths which are part of the system or equipment.

ay. Information Security. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information the protection of which is authorized by E.O. or statute.

az. Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, which concerns one or more aspects of foreign nations or of areas of foreign operations, and which is immediately or potentially significant to military planning and operations.

az.1 Letter of Consent (LOC) (DISCO Form 560). The form used by DISCO to notify a contractor that a Personnel Security Clearance (PCL) or a Limited Access Authorization (LAA) has been granted to an employee.

az.2 Limited Access Authorization (LAA). Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

az.3 Limited Dissemination (LIMDIS). Restrictive controls for classified *
information established by an original classification authority to *
emphasize need-to-know protective measures available within the regular *
security system. *

ba. Locked Entrance. A locked entrance is an entrance to a closed or restricted area which is kept closed and locked at all times except when temporarily unlocked and opened under supervision for the purpose of passing material or authorized personnel into or out of the area.

ba.1 Military Assistance Programs Address Directory (MAPAD). A *
printed listing of in-the-clear addresses for each country or international *
organization. The directory contains the addresses of country representatives, *
freight forwarders and customers-within-country required for releasing *
Foreign Military Sales (FMS) and Military Assistance Program (MAP) Grant Aid *
Shipments, and addresses required for forwarding of related documentation. *

bb. Material. Material refers to any product or substance on, or in which, information is embodied.

bc. Multiple Facility Organization (MFO). A legal entity (single *
proprietorship, partnership, association, trust, or corporation) that is *
composed of two or more facilities. *

bd. National of the United States. A national of the U.S. is:

(1) a citizen of the U.S., or

(2) a person who, though not a citizen of the U.S., owes permanent allegiance to the U.S. 2/.

be. National Security. This refers to the national defense and foreign relations of the U.S.

bf. NATO Classified Information. The term "NATO classified information" embraces all classified information -- military, political and economic -- that is circulated within and by NATO, whether such information originates in the organization itself or is received from member nations or from other international organizations.

bg. Need-to-Know. This is a determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to (see paragraph a above), knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a UA.

2/ See 8 U.S.C. § 1101(a)(22). 8 U.S.C. § 1401, subsection (a) lists in paragraphs (1) through (7) categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. When doubt exists as to whether or not a person can qualify as a national of the U.S., this subsection should be consulted.

bh. Negotiator. A negotiator is any employee, in addition to the OODEPs, who requires access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime or subcontract. (This category may include, but is not limited to, accountants, stenographers, clerks, engineers, draftsmen, and production personnel.)

bi. Nuclear Weapon Security Program. A limited number of defense contractors are involved in the DoD nuclear weapon security program. This program identifies certain positions categorized as Critical or Controlled, depending upon the degree of involvement with nuclear weapons. Assignment to such positions is governed by the DoD Nuclear Weapon Personnel Reliability Program (PRP), the specific procedures of which will be set forth separately in appropriate contractual agreements. All personnel in Critical or Controlled positions must have a security clearance required by their duties.

bj. Officers (Corporation, Association or Other Types of Business or Educational Institution). Officers are those persons in positions established as officers in the articles of incorporation or bylaws of the organization. This definition includes all principal officers; that is, those persons occupying positions normally identified as president, senior vice president, secretary, treasurer, and those persons occupying similar positions. In unusual cases, the determination of principal officer status may require a careful analysis of an individual's assigned duties, responsibilities, and authority as officially recorded by the organization. Excluded from this definition are: (i) assistant vice presidents who have no management responsibilities related to performance on classified contracts, (ii) assistant secretaries, and (iii) assistant treasurers.

bk. Reserved.

bk.1 Operations Security (OPSEC). The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. Section XV of this manual contains a detailed discussion of OPSEC and its relationship to industrial security.

bk.2 OPSEC Indicators. Actions or information (classified or unclassified), obtainable by an adversary, that would allow the adversary to develop or confirm assumptions, estimates and facts about U.S. intentions, military capabilities, plans, or programs, thereby compromising essential secrecy.

bl. Original Classification. This is an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

bl.1 Parent. A parent firm is a corporation that can control another corporation (subsidiary) by ownership of a majority of its stock. The control may exist by direct stock ownership of an immediate subsidiary or by indirect ownership through one or more intermediate levels of subsidiaries.

bm. Personnel (Security) Clearance (PCL). A PCL is an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the PCL being granted.

bn. Possessions. U.S. possessions are the Virgin Islands, Guam, American Samoa, Swain's Island, Howland Island, Baker Island, Jarvis Island, Midway Islands (this consists of Sand Island and Eastern Island), Kingman Reef, Johnston Atoll, Navassa Island, Swan Island, Wake Island and Palmyra Island.

bo. Principal Management Facility (PMF). A cleared facility of an MFO which reports directly to the HOF and whose principal management official has been delegated certain personnel security administration responsibilities or a defined geographical or functional area. The PMF will function as a Home Office Facility in relation to its area of responsibility. Both cleared and uncleared facilities may be under the jurisdiction of a PMF. (See paragraph 73 for approval requirements.)

bp. Protected Area. An area housing computer hardware used in the configuration and operation of an AIS which is continuously protected by a collective level of physical security safeguards and personnel access controls to prevent or detect unauthorized modification of the hardware.

bq. Protective Security Service (PSS). A transportation protective service provided by a cleared commercial carrier qualified by MTMC to transport SECRET shipments. The carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives and maintain a signature and tally record. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier's aircraft in connection with flight, provided the shipment is loaded into a compartment that is not accessible to any unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the aircraft that is accessible to an unauthorized person aboard, the shipment must remain under the constant surveillance of a cleared escort or qualified carrier representative.

br. Public Disclosure. Public disclosure is the passing of information and/or materials pertaining to a classified contract to the public, or any member of the public, by any means of communication.

bs. Qualified Carrier. A qualified carrier is a carrier that has met all of the following criteria.

(1) The requirement for the carrier's service has been established by a shipper.

(2) The carrier is authorized by law, regulatory body, or regulation to provide the required transportation service.

(3) A determination has been made by MTMC or the designated Commander overseas that: (i) the carrier is capable of and authorized to furnish PSS in accordance with an applicable tariff, government tender, agreement, or contract provision; and (ii) no other qualified carrier is available to perform the required service.

(4) The carrier has executed a DIS Form 1149, "Transportation Security Agreement," with, and has been granted a SECRET FCL by, the appropriate CSO.

bt. Reference Material. Documentary material over which the UA does not have classification jurisdiction, and did not have classification jurisdiction at the time such material was originated. Most material made available to contractors by the DTIC and other secondary distribution agencies is reference material as thus defined.

bu. Regrade. This is to assign a higher or lower security classification to an item of classified material.

bv. Remote Terminal. A remote terminal is a device for communication with an ADP system from a location, which is not within the central computer facility.

bw. Representatives of a Foreign Interest (RFI). This term refers to citizens or nationals of the U.S. or immigrant aliens who, in their individual capacities, or on behalf of a corporation (whether as a corporate officer or official, or as a corporate employee who is personally involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, or person. However, U.S. citizens and nationals who have been appointed by their U.S. employer to be its representatives in the management of a foreign subsidiary (that is, a foreign firm in which the U.S. firm has ownership of at least 51% of the voting stock) will not be considered RFI's, solely because of their employment, provided the appointing employer is their principal employer and is a firm that possesses or is in process for an FCL.

bx. Restricted Area. This is a controlled area established to safeguard classified material, which, because of its size or nature, cannot be adequately protected during working hours by the safeguards prescribed in paragraph 16, but which is capable of being stored during nonworking hours in accordance with paragraph 14 (see section II).

by. RESTRICTED DATA. "RESTRICTED DATA" is all data (information) concerning: (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the RESTRICTED DATA category pursuant to Section 142 of the Atomic Energy Act (see section 11y, Atomic Energy Act of 1954, as amended, and paragraph aq, FORMERLY RESTRICTED DATA, above).

bz. SECRET. "SECRET" is the designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security, significant impairment of a program or policy directly related to the national security, revelation of significant military plans or intelligence operations, compromise of significant military plans or intelligence operations, and compromise of significant scientific or technological developments relating to national security.

ca. SECRET Controlled Shipment. This refers to SECRET material moving in commercial transportation service that requires PSS of a qualified carrier in the interest of national security.

cb. Security. Security refers to the safeguarding of information classified TOP SECRET, SECRET, or CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

cc. Security Cognizance. This refers to the responsibility for acting for UA's in the discharge of industrial security responsibilities described in this manual.

cd. SENSITIVE COMPARTMENTED INFORMATION (SCI). This is all information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

ce. Shipper. A shipper is the one who releases custody of material to a carrier for transportation to a consignee (see also consignor, paragraph 3x.)

cf. Short Title. This is an identifying combination of letters and numbers assigned to a publication or equipment for purposes of brevity.

cg. Signature and Tally Record. A record that is an integral part of PSS and CSS and is designed to provide continuous accountability and custody of a shipment from point of pickup to delivery to the consignee. For commercial air shipments a signature is not required from the flight crew or attendees of the carrier's aircraft.

ch. Single Line Service. This refers to freight that moves from point of origin to destination over the lines of only one carrier.

ci. Special Access Program. A special access program is any program imposing "need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements, special designation of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know."

cj. Subsidiary. A subsidiary is a corporation that is controlled by another corporation (parent) by reason of the latter corporation's ownership of at least a majority (over 50%) of the capital stock. A subsidiary is a legal entity and shall be processed separately for an FCL.

cj.1 System Security Officer (SSO). The contractor person responsible for the implementation of AIS security, and operational compliance with the documented security measures and controls, at the contractor facility.

ck. System Software. Computer programs that control, monitor or facilitate use of the AIS, for example, operating systems, programming languages, communications, input-output control, sorts, security packages and other utility-type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics and computer-aided design.

ck.1 TEMPEST. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is often used synonymously for the term "compromising emanations," e.g. TEMPEST tests, TEMPEST inspections (See u.1, "Compromising Emanations," above).

cl. TOP SECRET. "TOP SECRET" is the designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the U.S. or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptologic and communications intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific or technological developments vital to national security.

cm. Transmission. Transmission is the sending of information from one location to another by radio, microwave, laser, or other nonconnective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

cm.1 Transportation Protection Service (TPS). A commercial carrier service performed according to DoD standards that provides intransit physical security for shipments of classified material. The two services used for shipments of SECRET and CONFIDENTIAL material are PSS and CSS, respectively.

cn. Transshipping Activity (Government). This refers to a government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

co. United States and Its Territorial Areas. This includes the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Trust Territory of the Pacific Islands (also called Micronesia), Midway Islands, Wake Island, Johnston Atoll, Kingman Reef, Swain's Island, Howland Island, Baker Island, Jarvis Island, Navassa Island, Swan Island, and Palmyra Island.

cp. Unauthorized Person. An unauthorized person is any person not authorized to have access to specific classified information in accordance with the provisions of this manual.

cq. United States (U.S.). This refers to the 50 states and the District of Columbia.

cr. Upgrade. This is a determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than is currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

cs. User Agencies (UA's). This term refers to the OSD (including all boards, councils, staffs, and commands), DoD agencies, Departments of the Army, Navy, and Air Force (including all of their activities), and Departments of: State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor and Justice, NASA, GSA, SBA, NSF, EPA, ACDA, FEMA, GAO, FRS, USIA, and USTR. *

ct. Weapon System. Weapon system is a general term used to describe a weapon and those components required for its operation.

4. Designation of Cognizant Security Office. The Regional Directors of DIS are responsible for administration of industrial security within their respective regions. The office of the Director of Industrial Security in each DIS Region is designated as the CSO for all contractor facilities located within the region (see appendix VIII). All relationships between the UA and the contractor on industrial security matters shall be handled through, or in coordination with, the CSO, except those matters specifically set forth in this manual as responsibilities of the contracting officer. All questions of interpretation with respect to this manual, or problems involving the industrial security procedures as they pertain to the contractor, shall be forwarded to the CSO. In the case of a facility or contractor activity located on a UA installation, requests for interpretations of this manual shall be forwarded to the CSO through the Commander or Head of the UA installation. The management of each facility that has been assigned to one of the DIS Regions for security cognizance shall be notified in writing of this action at such time as the DoD Industrial Security Program is initiated at the facility. The designation of CSO to exercise security cognizance at a facility will not relieve any UA of the responsibility for protecting and safeguarding its classified information incident to its classified contracts with the facility, or from visiting the facility to review the security aspects of such contracts. However, the security administration of a U.S. classified contract awarded to a U.S. contractor, which requires performance for a UA at a location outside the U.S., Puerto Rico, or a U.S. possession or trust territory shall be the responsibility of the UA awarding the classified contract, except when the contracting UA has an agreement with the U.S. installation Commander in such area to perform this function for it, or DIS has accepted responsibility at the request of the UA. The Director of Industrial Security in each DIS Region in which the HOF or principal U.S. based office of the contractor is located will assume security cognizance for such U.S. based facility, and except for contractor granted CONFIDENTIAL clearances, DISCO will clear all of the contractor's employees requiring access to classified information in support of a UA contract, regardless of the physical location of such employees. Contractor activities located outside the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory associated areas will not be granted an FCL.

5. General Requirements. The contractor shall be responsible for safeguarding all classified information under his or her control. In the furtherance of this requirement, the contractor will be responsible for the following.

a. Facility Security Officer/Supervisor (FSO). The contractor shall appoint a U.S. citizen, who is required to be cleared as part of the FCL, to supervise and direct security measures necessary for the proper application of U.S. Government furnished guidance or specifications for classification, downgrading, upgrading, and for safeguarding classified information. (A foreign national may serve as the FSO of a foreign-owned freight forwarder * facility. FSOs at freight forwarder facilities are exempt from the training * requirements as set forth below and specialized training will be provided by * the CSO.) The FSO, and those otherwise performing security duties, shall * complete security training as deemed appropriate by the CSO. Training for the FSO will be based on the facility's involvement in the DISP, and as a minimum will consist of the following:

(1) Facilities with no safeguarding capability: Satisfactory completion of the Essentials of Industrial Security Management (EISM) correspondence course within 6 months of obtaining an FCL or assuming security responsibilities.

(2) Facilities with safeguarding capability: Satisfactory completion of the EISM correspondence course within 6 months of obtaining an FCL or assuming security responsibilities and attendance at an Industrial Security Management Course conducted by the DoDSI within 12 months of acquiring safeguarding capability. Extensions to the 12 month requirement may be granted by the CSO when the Management Course is not available.

b. Automated Information System. The contractor shall not utilize an AIS system for the processing of classified data without the prior approval of the CSO (see section XIII).

c. Limitation on Disclosure. Contractors shall ensure that classified information is furnished or disclosed only to authorized persons (see paragraph 3e). To this end they shall determine to what extent their employees, subcontractors, vendors, and suppliers require access to classified information in the performance of tasks or services essential to the fulfillment of the contract 3/. They shall take all reasonable measures to adjust plant layout and organize work, so as to limit such access to the least number of individuals or firms consistent with the efficient performance of the classified contract.

3/ A contractor is not authorized to disclose or release classified intelligence information to a subcontractor, vendor, or supplier without prior written authorization of the contracting UA. All classified intelligence information, whether obtained during a visit or through other sources, shall be safeguarded and controlled in accordance with the provisions of this manual, as well as any additional instructions that may be received from the releasing UA activity and any specific restrictive markings or limitations appearing on documents. All inquiries concerning source, acquisition, use, control, or restrictions pertaining to intelligence information shall be directed to the contracting UA activity concerned.

d. Safeguarding. The contractor shall provide suitable protective measures within his or her facility for the safeguarding of classified information. A contractor performing work within the confines of a UA installation must safeguard classified information in accordance with provisions of this manual, unless responsibilities for security are modified by the contract. All classified material received by the contractor which: (1) is not related to a contract, project, or program pursuant to paragraph 1a, or (2) for which no safeguarding or disposition instructions have been received, shall be safeguarded in accordance with the provisions of this manual, and the CSO shall be notified pursuant to paragraph 6a(18).

e. Adverse Clearance Actions. In the event a contractor is notified by the DIS that a personnel security clearance concerning any of its OODEPs, employees, or consultants has been denied, suspended, or revoked, the contractor shall promptly preclude access to classified information by the affected individual. A case-by-case evaluation of the assigned duties and responsibilities of such affected individuals shall be undertaken to determine whether functional or physical reassignment will be necessary.

f. Individual Responsibility for Safeguarding. The contractor shall, on a recurring basis, remind all cleared personnel, including those located outside the U.S., of their continuing responsibilities for safeguarding classified information. Each cleared employee shall be made aware of the security procedures: (i) pertaining to that employee's particular work assignment; (ii) any security deficiencies resulting from recurring inspections by the CSO that require individual corrective action on the part of the employee; and (iii) shall be given an indoctrination in the methods and operations used by hostile intelligence services to subvert U.S. industrial personnel, as well as defensive measures to be employed by employees in order to counter such subversion. Part B of appendix VII provides indoctrination information on this subject. When representatives of the U.S. Government provide specific counterintelligence awareness briefings to the FSO, the FSO shall ensure that all cleared key personnel are also briefed, either at the time the FSO is briefed or at a subsequent briefing to be conducted by the FSO or designee. In addition, the employee who has possession or knowledge of classified information shall be informed that the employee is responsible for determining whether a prospective recipient is cleared and has a need to know. The employee shall be informed that he or she is required to advise the recipient of the classification of the information which he or she discloses. The contractor shall also inform its employees that unauthorized disclosure of classified information violates DoD regulations and contractual obligations, and is punishable under the provisions of federal criminal statutes. The employees shall also be informed of their responsibility for making certain reports to the FSO as specified in other paragraphs of this manual, such as, a change of name, becoming an RFI, personal exchanges with *
representatives of Designated countries, etc. *

g. Initial Security Briefings. Prior to permitting employees to have access to classified information, contractors shall brief them on their obligations to safeguard classified information, advise them of its importance, inform them of the required security practices and procedures, and have them read, or have read to them, the portions of the espionage laws, conspiracy laws, and federal criminal statutes applicable to the safeguarding of classified information, which appear in appendix VI of this manual.

(1) Following the initial security briefing the employee shall be required to execute the "Classified Information Nondisclosure Agreement," Standard Form (SF) 312 4/. The signature of the employee executing the SF 312 shall be witnessed by his or her supervisor or by another designated representative of the facility. Both signatures must bear the same date. The SF 312 must also be signed and accepted by a person empowered to act on behalf of the United States Government. The FSO is hereby specifically delegated the authority to accept, on behalf of the United States Government, the executed SF 312 for contractor employees. Further delegation of this authority is permitted in unusual circumstances provided that such delegations are in writing, specify the individuals who may accept the executions, and are made part of the facility's permanent security files. Only those individuals who occupy responsible positions within the facility's security system may be delegated such authority. In unusual circumstances, such as facilities with very few employees, a representative of the CSO or other government official may sign the acceptance portion of the form. The date of the acceptor's signature does not have to be the same as the date of execution.

(2) An employee shall be required to execute the "Security Debriefing Acknowledgment" portion of the SF 312 at the time of termination of employment (discharge, resignation, or retirement); at the beginning of a layoff or leave of absence for an indefinite period, or a prescribed period in excess of 120 days; if the employee's PCL is administratively terminated; if the employee's PCL is suspended or revoked by the DoD; and upon termination of the facility's FCL.

(3) The contractor shall retain the executed SF 312 for fifty (50) years from the date of the initial briefing, or for the duration of the FCL, whichever comes first. If a cleared operating location of an MFO ceases to be cleared, the SF 312 shall be forwarded to the HOF, if it continues to be a cleared facility. If the contractor's FCL is terminated, the SF 312 shall be forwarded to the CSO.

4/ The SF 312 and the SF 189-A are Nondisclosure Agreements between the United States and an individual. The prior execution of a least one of these Agreements, as appropriate, by an individual is necessary before that individual can be granted access to classified information. The effective date for use of the SF 312, in lieu of the SF 189-A, is September 29, 1988. However, an employee who signed the SF 189-A before or after September 29, 1988, shall be permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189-A and the contractor shall dispose of the superseded SF 189-A or indicate on it that it has been superseded. All cleared employees must execute a Nondisclosure Agreement as soon as possible but not later than December 31, 1989. Execution of the new form should be carried out in a manner that does not cause undue disruption in operations or contract performance and may be completed in conjunction with normal security actions, such as, required or recurring refresher briefings, or by use of batch distribution (by department, office, building, and the like). Contractors shall report to DISCO any refusal by a cleared employee to sign the SF 312 as required by paragraph 6b(11).

The SF 312s shall be maintained in such a manner that they can be expedi- *
tiously retrieved if required by the Government. In the interest of storage *
efficiency, contractors may place executed SF 312s on microfiche after the *
employee terminates employment. *

(4) If a terminating employee had access to TOP SECRET, COMSEC, *
or other information requiring a special access authorization by the U.S. *
Government, he or she shall be given an oral debriefing which shall include *
a statement of: (i) the purpose of the debriefing, (ii) the serious nature *
of the subject matter which requires protection in the national interest, *
(iii) the need for caution and discretion, and (iv) advice concerning any *
travel restrictions which are appropriate. *

h. Special Features of Design. Shall not incorporate any special features of design or construction in any project other than that for which they are furnished by, developed for, or designed for the Government, if such incorporation would disclose classified information unless prior written authorization of the contracting officer concerned has been obtained. However, classified features of design or construction may be incorporated by the contractor in other U.S. User Agency projects of equal or higher classification unless specifically prohibited by the Government. U.S. classified information shall not be used in the performance of a foreign classified contract unless the information was furnished through the designated military department in connection with that contract, or the U.S. contracting officer concerned has expressly authorized in writing the use of that information.

i. Security of Combinations. The contractor shall ensure that the combinations to safes, containers, vaults, and three-position dial-type changeable combination padlocks used to lock containers holding classified material are classified and safeguarded, in accordance with the highest level of the classified material stored in a given container. If a written record is established for the combinations, the record shall be marked with the classification designation of the highest level of material stored in the container. Other markings specified in paragraph 11 for classified material are not required. However, if the record is for the combination of a container used for storage of special categories of information, such as NATO, CNWDI, RESTRICTED DATA, or other information that requires special briefings or access requirements, procedures shall be established to ensure that the special requirements are adhered to and only those persons having a need-to-know are given access to the record of the combination. In addition, accountability for the written record shall be established in accordance with paragraph 12. The combinations shall be changed at intervals of at least once every year (if NATO or CRYPTO classified material is stored, the combination shall be changed every 6 months) and at the earliest practical time following:

(1) the reassignment, transfer, or termination of any person having knowledge of the combination; or

(2) when the PCL granted to any such person is downgraded to a level lower than the category of material stored, or is suspended or revoked by proper authority;

(3) the compromise or suspected compromise of the safes and containers or their combinations, or discovery of the container being left unlocked and unattended; or

(4) the initial receipt of safes, containers, and three-position dial-type changeable combination padlocks.

Combinations to safes, containers, vaults, and three-position dial-type changeable combination padlocks shall be changed under the above schedule by a person entrusted with the combination or authorized access to the contents of the container in accordance with paragraph 14c, or by the FSO or his or her designated representative. Under no circumstances shall the changing of the combinations be performed by an outside locksmith or subcontractor employee. To prevent unauthorized substitution, combination padlocks shall be placed inside of the open container or secured to a hasp, drawer, or handle of the container when it is open.

j. Security Checks. The contractor shall perform security checks within the facility to ensure that at all times security precautions are taken to protect classified material in the possession of the facility and shall designate an individual or individuals to make room or area checks during normal working hours to ensure that all classified material not under surveillance has been properly stored.

k. Transmission. The contractor shall establish procedures for the proper transmittal of classified material under the provisions of paragraph 17. A freight forwarder shall include a transportation section in his/her SPP prepared in accordance with paragraph 5s. *

l. Disposition of Classified Material. The contractor shall return to the contracting officer, or his or her designated representative, all classified material furnished by a UA, including all reproductions thereof, and shall surrender all classified material developed by the contractor in connection with a UA contract, program, or solicitation 5/ 6/, unless the material has been destroyed in accordance with paragraph 19, or the retention of the material is authorized under the provisions of paragraph m below. Such material shall be returned or surrendered in accordance with the following schedule:

(1) if a bid, proposal, or quote is not submitted or is withdrawn -- within 90 days after the opening date of bids, proposals, or quotes;

(2) if a bid, proposal, or quote is not accepted -- within 90 days after notification that a bid, proposal, or quote has not been accepted and if further retention is necessary to serve a UA purpose, a request for approval shall be submitted to the appropriate contracting officer in accordance with paragraph m below; or

---

5/ The placing of an appropriate notation on each document, indicating the specific contract to which it pertains, will assist in achieving compliance with this paragraph.

6/ Classified material, which is not related to a proposal or classified contract (see paragraph 1a), may be destroyed in accordance with the provisions of paragraph 19c (unless specifically prohibited), or disposed of in accordance with instructions issued by the UA that originally furnished the material.

(3) if a successful bidder -- on final delivery of goods or services, or on completion or termination of the contract, unless otherwise prescribed in the contract or directed by the contracting officer.

m. Retention of Classified Material

(1) The contractor may retain classified material in special cases when a bid, proposal, or quote is not accepted or upon completion or termination of the contract provided the contractor requests and justifies such retention and its retention is agreed to by the contracting officer. The contractor shall be authorized to retain classified material only: * * * * *

(a) when retention is necessary for the maintenance of the contractor's essential records;

(b) when classified information is also patentable or is proprietary data in which the contractor has title; or

(c) when retention of the material will assist the contractor and will benefit the U.S. Government in the performance of other UA contracts (the contracting officer of a current classified contract may authorize transfer of the material to the current contract when the material is identified by the contractor in accordance with the procedure set forth in paragraph 5m(1)(d) 7/ -- in these situations the material will be disposed of, in accordance with paragraph 5l, at the completion of the current contract); and

(d) when the contractor justifies and requests retention authority in writing, indicates the period of time retention is necessary, and identifies the classified material for which retention is requested as follows: TOP SECRET and SECRET material shall be identified in a list of specific documents unless, in the case of SECRET material only, the contracting officer has authorized identification by subject matter and approximate number of documents; CONFIDENTIAL material shall be identified by subject matter and approximate number of documents. However, authorization of the contracting officer is not required for the retention of: (i) records held by the contractor in accordance with the records retention requirements of the basic contract; (ii) records authorized for retention for a specific period under the terms of the basic contract; and (iii) records which during the contract period, the contracting officer authorized the contractor to

---

7/ When such approval is granted the contracting officer who has cognizance over the classified material shall be notified by the current contracting officer. In the event retention of information under the circumstances contemplated in this paragraph involves information of a DoD UA being retained by a contractor of a non-DoD UA, or vice versa, or between non-DoD agencies, the concurrence of the contracting officer of the completed or terminated contractor bid which was not accepted must be obtained by the current contracting officer prior to authorizing retention of the materials. Information authorized for retention under these circumstances will be identified as to its origin, and its ultimate disposition or declassification will remain with its originating agency.

retain for a specific period following completion of the contract; provided that in each case the contractor informs the contracting officer of the material to be retained, identifying it in the manner prescribed above.

(2) The contractor may retain classified material which does not relate to a contract, for a limited time unless indicated otherwise on the material. For example, the contractor may retain material obtained at classified symposiums or meetings as long as needed, but not for a period to exceed 1 year from the date of receipt. Retention beyond that time is authorized only when the contractor requests and justifies such retention, and retention is agreed to by a contracting officer of a current contract or an official of the UA which released the information.

n. Termination of Security Agreement. The contractor shall, notwithstanding the provisions of paragraphs l and m above, in the event that the DD Form 441 is terminated for any reason by either party and is not superseded by a new DD Form 441, render all classified material in his or her possession to the UA concerned, or dispose of such material in accordance with instructions from the UA concerned. The DIS FL 381-R, "Letter of Notification of Facility Security Clearance," and the contractor's copy of the DD Form 441 or the DD Form 441-1 (or DIS Form 1149 and DIS Form 1150, as appropriate) shall be returned to the CSO. Control station records, reproduction records, destruction certificates, and visitor records for which the retention period is not expired at the time of termination of the DD Form 441, shall continue to be maintained by the contractor until the expiration of the prescribed retention period. These records shall be subject to review and recall by the U.S. Government at any time within the retention period.

o. Public Disclosure. Contractors shall not disclose information 8/ pertaining to classified contracts or projects, except as specified in paragraph (2) below, without prior review and clearance of the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs), 9/ (OASD(PA)), The Pentagon, Washington, D.C. 20301, in order to preclude the disclosure of information requiring protection in the interest of national security.

(1) Requests for clearance shall be submitted to the activity specified in item 13 of the Contract Security Classification Specification

---

8/ In addition to the requirements of this paragraph, the disclosure of unclassified technical data is also governed by the Export Administration Act of 1979, administered by the Secretary of Commerce through the EAR, and the Arms Export Control Act of 1984, administered by the Secretary of State through the ITAR.

9/ If the information pertains to a classified contract or project awarded by a non-DoD agency, requests for clearance to disclose shall be submitted to that agency.

(DD Form 254). Each request for clearance shall indicate the approximate date the contractor intends to release the information for public disclosure and identify the media to which he/she intends to make the initial release. A copy of each request that is approved for release shall be retained for a period of one inspection cycle for review by the CSO. All information developed subsequent to the initial clearance shall also be cleared by the OASD(PA) prior to public disclosure.

(2) Contractors performing on DoD classified contracts need not submit for clearance the following information:

(a) The fact that a contract has been received, including the subject matter of the contract, and/or type of item in general terms provided the name or description of the subject matter is not classified.

(b) The method/type of contract; that is, bid, negotiated, letter, etc.

(c) Total dollar amount of the contract unless that information equates to, (i) a level of effort in a sensitive research area, or (ii) quantities of stocks of certain weapons and equipments which are classified.

(d) Whether the contract will require the hiring or termination of employees.

(e) Other information which from time to time may be authorized on a case-by-case basis by the OASD(PA) in a specific agreement with the contractor.

(f) Information previously officially approved for disclosure by OASD(PA).

(3) The provisions of this paragraph also apply to information pertaining to classified contracts or projects intended for use in unclassified brochures, promotional sales literature, reports to stockholders or similar type material. In case of doubt about the need to clear information, contractors shall query the activity identified in item 13 of the DD Form 254 or the OASD(PA).

p. Classified Sales Literature. The contractor shall not publish or distribute, or permit to be published or distributed, brochures, promotional sales literature, or similar material containing classified information, without prior review and written authorization by the contracting officer concerned or his or her designated representative. The authorization for such publication and distribution shall be indicated on the cover of the document, or the first page of the document, if there is no cover. However, publication and distribution to authorized persons (see paragraph 3e) may be made without specific authorization from the contracting officer for:

(1) classified material which is published or distributed for necessary use within the organization of the contractor or his or her subcontractor in the performance of the contract;

(2) classified material prepared in reply to a request for proposal or invitation to bid received from a UA or a cleared prime contractor or subcontractor of a UA or classified information contained in an unsolicited proposal submitted to a UA; and

(3) classified material submitted in response to an official request of a UA.

q. Disclosure at Meetings. The contractor shall not disclose in any manner classified information at a conference, seminar, symposium, exhibit, or convention (hereinafter referred to as a meeting), unless one of the following conditions is met.

(1) Classified information may be disclosed at a meeting conducted pursuant to, and as a necessary element of, a specific contract held only in the prime or subcontractor's facility and attended only by authorized persons who have a need-to-know in connection with the contract, including employees of the contractor or subcontractors, consultants thereto, and authorized visitors, and over which meeting controls have been established to ensure that the meeting site is physically secure, that the classified notes, minutes, and summaries resulting from the meeting are properly safeguarded and that the attendees are given sufficient classification guidance during the oral presentations.

(2) Classified information may be disclosed at a meeting conducted by a DoD activity, provided that when the information to be disclosed is under the jurisdiction of another U.S. Government agency or when the meeting is to be attended by representatives outside the DoD, the contractor requests the conducting activity to obtain written approval from the contracting officer concerned prior to the disclosure. A copy of such request shall be furnished to the contracting officer concerned. The contractor is not required to obtain approval if only DoD information is to be disclosed, and only the contractor, subcontractors and their employees, and DoD personnel are to attend the meeting.

(3) Classified information may be disclosed at a meeting conducted by a contractor, association, institute, or society whose membership is comprised primarily of contractors cleared by DoD, contractor employees, or DoD personnel, and sponsored for security purposes by the DoD (including the departments and agencies named in paragraph 1c), provided written approval of the contracting officer concerned is furnished to the sponsoring activity prior to the disclosure, and the additional requirements of paragraph 9 are fulfilled; or

(4) Classified information may be disclosed at a meeting conducted or sponsored by U.S. Government agencies other than DoD, provided the contractor requests and obtains written approval from the contracting officer concerned prior to the disclosure. Security sponsorship of a meeting by a UA other than DoD will be in accordance with the provisions of that agency. However, as a minimum, the requirements of the ISM shall apply for the safeguarding of classified information.

r. Controlled Areas. The contractor shall place in effect a system to control access of employees and visitors to closed and restricted areas (see section IV).

s. Standard Practice Procedure (SPP). Prior to the issuance of an FCL by the CSO, the contractor shall submit a written SPP (interim or final) in sufficient detail to place into effect all security controls required by the DD Form 441 and this manual which are applicable to the operations of the facility. An interim SPP must implement requirements of this manual which are immediately applicable to the operations of the facility in connection with the facility's anticipated involvement with classified information. The contractor shall modify the SPP on notification from the CSO that it does not adequately implement the requirements of this manual. The SPP shall be revised when necessary to implement changes in the contractor's operations and shall be revised as necessary within 4 months after receipt of a revision to this manual.

(1) MFO's, or parent-subsidiary collocated facilities, may publish an SPP applicable throughout the organization, but the SPP shall then be adapted as necessary to apply to specific operating locations. A copy of the SPP shall be furnished to each appropriate CSO.

(2) The SPP for a facility at which only one employee or management official is assigned shall provide for the notification to the CSO of the death or incapacitation of that employee. Specifically, the SPP shall:

(a) identify by name, address, and telephone number, the individual(s) who would notify the CSO of such an occurrence (the said individual(s) would not require access to classified information and therefore need not be cleared); and

(b) include provisions for keeping the CSO advised of the current combination to the container or, in the case of one-person facilities of an MFO, for keeping the HOF FSO advised of the current combination to the container.

(3) The SPP prepared by a freight forwarder shall specify the storage facilities, delivery and transfer points, carriers, couriers, or escorts, and methods of handling from the CONUS point of origin to the final destination. *

t. Special Access Programs. The contractor shall implement special access program requirements when such requirements are included in a DD Form 254 or other appropriate contract-related document.

u. Defensive Security Briefing.

(1) The contractor shall require all cleared employees (including cleared OODEPs), Type A Consultants, and temporary help supplier *

personnel, to inform him or her of (i) any personal exchange 10/ with nationals or representatives of Designated countries; (ii) intended travel to or through a Designated country; (iii) attendance at an international scientific, technical, engineering, or other professional meeting, regardless of the geographic location of such a meeting, when it can be anticipated that representatives of Designated countries will participate or be in attendance; or (iv) plans to host a visit by representatives of Designated countries at a facility engaged in a classified contract. Employees of a temporary help supplier must report such information to their employer(s) and to the contractors and/or UA's using their services. If only one cleared person is assigned to a facility that person shall report to the CSO.

(2) The contractor shall administer a defensive security briefing to the individual using the guidance contained in appendix VII. Where multiple employers or duty stations are involved, only one contractor or UA is required to accomplish the briefing. Evidence of the administration of the briefing must be documented and furnished to all other employers, as appropriate. Individuals who have a continuing personal exchange with the same individual, frequently travel, attend meetings, or host visits as described above need not be briefed on each such occasion provided the individuals have been thoroughly briefed at least once within the preceding 6 months and reminded of their security responsibilities. Prior to departure of personnel for travel to or through a Designated country or to attend a meeting outside the U.S., all classified material in the custody of such personnel shall be accounted for. Cleared and uncleared employees expected to engage in marketing activities with representatives of Designated countries shall also be provided with a defensive security briefing based on the guidance contained in appendix VII.

(3) The contractor shall, on completion of the briefing, obtain from the individuals briefed, statements identifying who furnished the briefing and attesting that they understand their individual responsibilities for safeguarding classified information. This statement shall be retained for at least 3 years when an employee has had access to TOP SECRET, COMSEC, or special access program information, and for at least 2 years when access has been to SECRET or CONFIDENTIAL information. In the case of temporary help supplier personnel, the statement shall be forwarded to the temporary help supplier for retention. If the UA or CSO conducts the briefing, it is responsible for obtaining the briefing statement.

(4) The contractor shall submit a report as required by paragraph 6b(9) unless the UA or CSO conducted the briefing, in which case the UA or CSO will submit the report.

10/ A personal exchange is defined as an encounter, either in person or in writing whereby, as a minimum, the identity and occupation of the parties become known to each other. The term includes business relationships. If an employee has had contact with such persons and is not sure of the applicability of this requirement, he or she shall seek advice and counsel by furnishing full particulars to the FSO or his or her designee for this purpose.

v. Relationships with Citizens or Residents or Designated Countries.

(1) The contractor shall require all cleared employees, including those in the process of being cleared by the DoD, to immediately notify the contractor who shall submit a report to DISCO, in accordance with paragraph 6b(4), if either or both of the following events should occur subsequent to the completion of the employee's PCL forms:

(a) a member of the immediate family of the employee or the employee's spouse takes up residence in a Designated country; or

(b) through marriage, the employee acquires relatives who are citizens or residents of a Designated country.

(2) The contractor shall require all temporary help supplier personnel, while such personnel are working under the contractor's direction and control on the using contractor's classified programs or contracts, to notify the contractor immediately if either or both of the events in paragraphs (a) and (b) above should occur. In such a case, contractors shall then take action to ensure that the temporary help suppliers are notified so that they can take action to submit reports to DISCO in accordance with paragraph 6b(4).

w. Emergency Procedure. Contractors shall include in their SPP general instructions for safeguarding classified material in emergency situations, such as natural disasters or any civil disturbances. The procedure shall be as simple and practical as possible and should be adaptable to any type of emergency that may arise. A procedure shall be incorporated in the SPP to provide for the submission of a report to the CSO and contracting officer, by the most expeditious means, of any emergency situation which renders the facility incapable of safeguarding the classified material (see paragraph 6a(16)). Courses of action, not necessarily limited to the following, are available to contractors to safeguard the classified material in their possession.

(1) Secure the classified material in authorized storage containers or controlled areas. If feasible, a guard(s) should remain with material secured in controlled areas. The storage containers and controlled areas shall be examined on return to the facility to determine whether the classified information has been compromised or if any classified material is missing. A report shall be submitted in accordance with paragraph 6a(1) or (2), if appropriate.

(2) Request assistance from appropriate civil authorities including local and state law enforcement agencies.

(3) Seek legal remedies such as the issuance of a court restraining order or injunction against interference with the contractor in the exercise of his or her property rights or in the discharge of his or her contractual obligation to safeguard classified information.

(4) Request, when necessary, the assistance of the CSO; for example: (i) in obtaining the legal remedies described in paragraph (3) above, and (ii) in arranging for the removal and safekeeping of the classified material by either the CSO, contracting activity, or a military activity located at or near the facility.

x. Release or Transmission Outside Contractor's Facility. The contractor shall obtain the approval of the contracting officer in every instance prior to release or transmission of TOP SECRET information outside a contractor's facility. With respect to SECRET and CONFIDENTIAL information, the contractor shall obtain the contracting officer's approval for release or transmission outside the contractor's facility except in the following instances:

(1) when release is required by the specific terms of the contract;

(2) when it is necessary in the performance of the contract;

(3) in connection with precontract negotiations with prospective subcontractors, vendors, or suppliers;

(4) in prime contractor-subcontractor, MFO, and parent-subsidiary relationships as authorized by sections VI and VIII, respectively; and

(5) during visits among prime contractors which are participating under U.S. Government direction in contracts pertaining to research, development, or production of a weapon system (see paragraph 3ct).

When a contract requires classified material to be disseminated by a contractor to another contractor in accordance with a standard mailing or distribution list, and there is no current contractual relationship of a classified nature between the contractor and a designated recipient, the releasing contractor shall verify the FCL and safeguarding ability of the recipient prior to making the first release of any material, except when advised by the contracting activity supplying the distribution list that it will retain the responsibility for these determinations. If appropriate, the CSO of the recipient shall be advised by the releasing contractor that classified material will continue to be disseminated to the recipient under terms of the contract (identify the contracting activity and contract number) for a specified period (not to exceed the estimated date of contract completion or renegotiation), unless advised by the CSO of a change adversely affecting the recipient's FCL or safeguarding capability. When the mailing or distribution list requires dissemination of the material to a UA installation, the foregoing requirements do not apply, but the material shall be transmitted in accordance with paragraph 17.

y. DoD Technical Information Dissemination Activities. The contractor shall forward the DD Form 1541, "Facility Clearance Register," to the CSO when making the first application for access to classified scientific and technical information in the possession of the DTIC (Cameron Station, Alexandria, Virginia 22304), its field extensions, a DoD information analysis center, or the Redstone Scientific Information Center (U.S. Army Missile Command, Redstone Arsenal, Alabama 35898-5238). This form is used to obtain certification of the category of classified material that an applicant (contractor) is cleared to receive and is capable of safeguarding. A DD Form 1541 shall be submitted only when requesting approval of the first "Registration for Scientific and Technical Information Services" (DD Form 1540). When certified, the DD Form 1541 remains in effect for all future registrations and until the contractor's FCL is suspended, revoked, or terminated, or until the contractor is no longer able to safeguard classified material at the specified category. The DD Form 1540 shall be submitted to the sponsoring UA contracting officer, in accordance with guidance provided by DTIC. Scientific and technical information acquired from DTIC, its field extensions, a DoD information analysis center, or the Redstone Scientific Information Center shall be safeguarded in accordance with the requirements of this manual and the restrictions on the use, disclosure, and dissemination of the information, which are marked on the documents. When the contract to which the DD Form 1540 applies is completed or terminated, the contractor shall either destroy the material in the manner prescribed in paragraph 19 or obtain authorization to retain the documents from the sponsoring UA in accordance with paragraph 5m. The placing of an appropriate notation on each document, indicating the specific contract to which it pertains, will assist in achieving compliance with this requirement.

z. Reserved.

aa. Official Assistance and Cooperation. The contractor shall cooperate fully with representatives of DIS or other federal investigative agencies during official inspections, investigations concerning the handling * of classified information, and during the conduct of investigations related to determining the eligibility of past or present employees or other personnel requiring a security clearance. This includes, but is not limited to providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, making employment and security records available for review on request by such representatives, and otherwise rendering assistance as necessary.

ab. Temporary Help Supplier Personnel. The contractor shall orient temporary help supplier personnel in the security practices and procedures of the facility, which will enable such personnel to understand and comply with the procedures applicable to the duties they are to perform. Using contractors will also submit, as appropriate, reports pertaining to such personnel while they are actually working at their facilities under their direction and control. This action by the using contractor in no way relieves the temporary help suppliers from complying with the requirement for security indoctrination and training of their employees or other concurrent requirements of this manual.

ac. Self-Inspections. Contractors shall conduct their own self-inspection program for the purpose of evaluating all security procedures applicable to the facility's operation. Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection to occur midway between inspections conducted by the CSO. At the discretion of management, the inspection may be conducted by a security representative(s) from the facility, HOF, PMF, or cleared parent. In any event, management shall establish, at an appropriate organizational level, a procedure for evaluating the effectiveness of the self-inspection program. Self-inspection shall consist of an audit of all the facility's operations in light of its SPP and the requirements of this manual. As a minimum, self-inspections shall include all elements normally inspected by the CSO. The guidelines used by U.S. Government inspectors are outlined in appendix XIII. These guidelines will change from time to time to reflect changes in ISM requirements. Not all of the items listed in appendix XIII are intended to be covered during any one inspection, but over a reasonable period of time those items that pertain to a facility shall be covered during the self-inspections. Deficiencies identified as a result of self-inspections shall be corrected as expeditiously as possible. If difficulty is encountered in resolving a deficiency, the CSO will provide assistance on request. The contractor shall maintain a record of the date on which the self-inspection was accomplished, and this record must be available for review during the next scheduled inspection by the CSO.

ad. Classification Responsibilities of Contractors. The contractor is responsible to implement the classification decisions of the U.S. Government contracting authority. Contractor implementation shall be based on classified source material or a DD Form 254 with its enclosed or referenced classification guides.

ae. Verification of U.S. Citizenship. The contractor shall require each employee who is an applicant for a PCL (including the "CONFIDENTIAL" level) and who claims U.S. citizenship to produce evidence which will verify such citizenship. Documents which are acceptable evidence of U.S. citizenship are listed at appendix XII. Unless the form has a verification block, a statement as follows will be typed or stamped by the contractor in the "Remarks" portion of the appropriate DoD clearance forms: "Authorized evidence of U.S. citizenship has been reviewed by the certifying official and the name, date, and place of birth therein are as stated on this form." (The recent revisions of DD Forms 48 and 49 have included verification blocks added to the forms.) In the case of PCL's by the DoD, if the required documentary evidence is not immediately obtainable prior to submission on the application to DISCO, a statement as follows will be typed or stamped in the "Remarks" portion of the appropriate DoD clearance form: "Applicant has applied to (insert name of agency organization) for authorized evidence of citizenship (insert acceptable document from appendix XII)." On receipt of evidence of citizenship, the contractor will notify DISCO that authorized evidence of U.S. citizenship has been reviewed and that the name and date and place of birth are as stated in the previously submitted clearance form. DISCO will not forward an LOC until the contractor has certified the applicant's U.S. citizenship. CONFIDENTIAL clearances by the contractor shall be granted in accordance with paragraph 24b.

af. Supervisory and Managerial Responsibility for Reporting Adverse Information. Supervisory and managerial personnel shall be reminded of their responsibilities for advising the FSO of the existence of any information coming to their attention concerning any employee who has been cleared or is in the process of being cleared for access to classified information, when information indicates that such access may be questionable or not in the interest of national security.

ag. Security Inspections. As provided for in Section II of the *
"Department of Defense Security Agreement," security inspections of cleared *
contractor facilities will be conducted by the CSO in order to ensure that *
the procedures, methods, and physical safeguards employed by contractors are *
adequate for the protection of classified information entrusted to them. In *
conducting these inspections, representatives of the CSO will, in part, *

review records maintained by the contractor, interview employees of the contractor, assess the adequacy of the contractor's system of security controls, and ensure compliance by the contractor with all applicable terms of this manual. At the discretion of DIS, employee interviews will be conducted in private between the employee and the DIS representative in order to create an environment which will allow for the freest exchange of information. Security inspections necessarily subject all areas, rooms and receptacles under control of the contractor to physical examination. Physical examination of the interior space of desks, cabinets and similar office equipment not authorized to secure classified material will normally be limited to periodic spot-checks. However, these spot or random checks will be expanded when there is reason to believe that classified material may have been improperly stored, such as when classified material has been discovered improperly stored elsewhere in the facility. In the conduct of these inspections, every effort will be made to avoid unnecessary intrusion into the personal effects of contractor personnel. Moreover, the CSO's physical examination of the interior space of equipment not authorized to secure classified material will be accomplished, whenever possible, in the presence of the individual responsible for the equipment, and such inspections will always be accomplished in the presence of a representative of the contractor. The frequency of general inspections by the DoD is normally determined by the highest level of classified material possessed at the facility. The CSO will normally advise the contractor when these inspections will be conducted. However, security inspections may be conducted on an announced or unannounced basis. On a random basis, the CSO will also conduct periodic inspections of uncleared locations of the contractor at which cleared employees are assigned. When receiving notice of a forthcoming inspection, the contractor shall prepare a listing of all classified contracts on which the facility is currently performing.

ah. Reserved.

ai. Operations Security. The contractor shall comply with OPSEC requirements when such requirements are contractually imposed by UA's. In meeting OPSEC requirements, contractors shall identify implementation costs to UA's and shall assist UA's in determining existing ISM measures which address particular UA vulnerability concerns in order to preclude the imposition of duplicate OPSEC measures. Additional costs for OPSEC provisions required by the UA shall be properly charged to specific contracts. See Section XV of this manual for further discussion.

aj. Administrative Measures Regarding Security Violations. The contractor shall establish and enforce policies which provide for appropriate administrative actions against employees who violate requirements of this manual. The SPP shall include a graduated scale of disciplinary actions which would be applied by the contractor in the event of such employee violations or negligence. When contractors submit reports in accordance with paragraphs 6b(1) or 7(e) with regard to culpable individuals responsible for a security violation, a statement as to the administrative actions taken against the individual shall be included. If the action is different from that specified in the SPP, an explanation shall also be included.

ak. Defense Hotline. The Defense Hotline provides an unconstrained avenue for DoD personnel and contractor employees to report, without fear or reprisal, known or suspected instances of serious security irregularities and infractions concerning defense affiliated contracts, programs, or projects. The Defense Hotline does not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels. However, the Hotline may be used as an alternate means to report this type of information when considered prudent or necessary. The Defense Hotline is organized and administered by the Office of the Inspector General, DoD. That office initiates investigative action regarding information received through the Hotline system and has primary responsibility for ensuring the confidentiality of all system users. The contractor shall conspicuously post publicity media provided by DIS regarding the Defense Hotline and shall inform all employees that the Hotline may be used, if necessary, for reporting matters of national security significance. The address, telephone number, and purpose of the Defense Hotline shall be included in the SPP. The address and telephone number are:

Defense Hotline
The Pentagon
Washington, D. C. 20301-1900
800-424-9098 (toll-free)
(202) 693-5080 (Washington, D. C. Metro area)

al. TEMPEST Requirements. TEMPEST protective measures may be required for certain contracts which involve processing classified information by information processing equipments. Contractors are required to comply with TEMPEST requirements, such as providing data to a UA for a TEMPEST Vulnerability Assessment and/or Instrumented TEMPEST Survey, or taking specific TEMPEST countermeasures, only when these special security requirements are specifically incorporated into the contract. These requirements are above and beyond those normally called for in this manual and may be cause for renegotiation in accordance with the "Security Requirements Clause" of the contract. Contractors shall not implement specific TEMPEST countermeasures nor shall they impose any TEMPEST requirements on a subcontractor without prior approval of the UA contracting office. The CSO may be contacted for advice and assistance when questions or problems arise.

am. Perimeter Controls. Contractors authorized to store classified material shall establish and maintain a formal system to deter and detect unauthorized introduction or removal of classified material from their facility. The purpose of this requirement is to form a credible deterrent to employees and visitors to prevent unauthorized introduction or removal of classified material without proper authority. If the unauthorized introduction or removal of classified material can be reasonably foreclosed through technical or other means, the perimeter control requirements prescribed herein do not apply. Employees who have a legitimate need to remove or transport classified material shall be provided appropriate authorization media for passing through designated entry/exit points. The fact that persons who enter or depart the facility are subject to an inspection of their personal effects shall be conspicuously posted at all pertinent entries and exits.

(1) All persons who enter or exit the facility shall be subject to an inspection of their personal effects, except under circumstances where the possibility of access to classified material can be reasonably

foreclosed. If feasible, inspections shall be limited to buildings or areas where classified work is being performed. Inspections shall be limited to that necessary to determine whether classified material is (i) contained in briefcases, shoulder bags or handbags, luggage, athletic bags, packages and the like, and whether such material is (ii) being improperly removed from or taken into the facility. Inspections are not required of wallets, change purses, clothing, cosmetics cases, or other objects of an unusually personal nature.

(2) Inspections may be conducted at irregular intervals and shall be implemented in a manner which does not interfere unduly with contract performance or facility operations. They may be accomplished at one or more designated entry/exit points and need not be carried out at all such points concurrently. Inspections may be done on a random basis using any appropriate sampling technique. They may be limited, based on time-of-day, shift changes, nature of work, and the like. For example, during a peak period of pedestrian traffic, a limited sampling of personnel may be employed whereas a 100 percent inspection may be desirable at the same entry or exit point during a period of sparse traffic. Similarly, an inspection of the personal effects of a single employee over a period of several months could satisfy the credible deterrent standard given existing controls and a particular set of circumstances. The method and frequency of inspections of personal effects at entry and exit points shall be at the discretion of the contractor. Contractors are encouraged to seek legal advice during the formulation of implementing procedures and to surface significant problems to the CSO.

an. Transportation Plan/Transmission Instructions. Each contract, agreement, or other arrangement that involves the release of classified material to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials prior to release of the material. Defense contractors will consult, as appropriate, with the purchasing government, the DIS CSO, and the owning military department prior to consummation of a contract that will result in the shipment of classified material, to obtain approval of the transportation plan or transmission instructions. Transmission instructions or the requirement for an approved transportation plan on FMS shall be specified and incorporated into the security requirements of the "United States Department of Defense Offer and Acceptance" (DD Form 1513). Appendix XVII contains specific requirements to be included in a transportation plan/instructions. Unless the transportation plan or instructions are approved as submitted, or modified to meet U.S. security standards, shipment by other than the Defense Transportation System (DTS) shall not be permitted.

ao. Limited dissemination. LIMDIS protective measures may be contractually imposed, for a specified period of time, by a DoD UA to safeguard particularly sensitive classified information. Once a LIMDIS determination has been made, evidence of that determination and the requisite additional protective measures to be applied will be included on the DD Form 254. The term "LIMDIS" does not pertain to additional security controls imposed pursuant to an approved Special Access Program. Contracts that include LIMDIS controls are under the security cognizance of the DIS.

6. Reports.

a. The contractor shall immediately submit in writing to the CSO a report of any of the following 11/.

(1) Espionage, Sabotage, or Subversive Activities. The contractor shall submit an information copy of any report filed under paragraph 6c with the FBI.

(2) Loss, Compromise, or Suspected Compromise. The contractor shall submit a report, classified if appropriate, of any loss, compromise (including deliberate compromise), or suspected compromise of classified information 12/.

(3) Other Security Violations. In addition to the requirement of paragraph a(2) above, the contractor shall submit a report, classified if appropriate, of each violation of the requirements of this manual involving TOP SECRET or special access information, RESTRICTED DATA, or COMSEC information, regardless of classification, which the contractor possesses in connection with UA contractors or programs 12/. The contractor's preliminary and/or final reports shall contain the information required by paragraphs 7c and 7e, respectively.

(4) Changed Conditions.

(a) The contractor shall submit a report of any change of ownership, including stock transfers, that affect control of a corporation.

(b) The contractor shall submit a report of change of operating name or address of the facility(s) covered by the DD Form 441.

11/ When reports are submitted or information is provided pursuant to these requirements, either classified if qualified, or offered in confidence, and so marked by the contractor, applicable exemptions to the Freedom of Information Act will be invoked as a matter of policy to withhold the information contained in such reports from public disclosure. When any of the reports submitted pursuant to these requirements contain unclassified information pertaining to an individual, the Privacy Act of 1974 permits the withholding of that information from that individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the U.S. Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. In appropriate cases, the DoD will entertain a request from a defense contractor or its employees for such assistance as may be necessary against legal action based on the reporting of information in accordance with the requirements of this manual. Such assistance may include support for a claim by the contractor or the employees concerned that the information was reported under an absolute or qualifying privilege. In such cases, the DoD will request appropriate assistance from the Department of Justice.

(Footnote 12/ is on the following page.)

(c) The contractor shall submit a report of any change (that is, additions, deletions, or any change relative to the information which was previously submitted) in officers, directors, partners, regents, trustees, or executive personnel, including, as appropriate, the names of the individuals they are replacing. In addition, a statement shall be made indicating: (i) whether the new officers, directors, partners, regents, trustees, or executive personnel are cleared, and if so, to what level and when, their date and place of birth, social security number, and their citizenship; (ii) whether they have been excluded from access in accordance with the provisions of 22e; (iii) or whether they have been temporarily excluded from access pending the granting of their PCL's. A new complete listing of OODEPs need only be submitted at the discretion of the contractor and/or when requested in writing by the CSO.

(d) The contractor shall submit a report about any OODEP who becomes an RFI, as defined in paragraph 3bw, or whose status as an RFI changes in a manner that would make the OODEP ineligible for a PCL pursuant to paragraph 20k.

(e) The contractor shall submit a report of action to terminate business for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the DD Form 441.

(f) The contractor shall submit a report of any change which affects the information previously reported by the contractor on the DD Form 441s, "Certificate Pertaining to Foreign Interests." This report shall be made by the submission of a revised DD Form 441s. Moreover, when entering into discussions or consultations with foreign interests which may reasonably be expected to lead to the introduction or increase of FOCI and necessitate the submission of a revised DD Form 441s, the contractor shall * report the details by letter. Additionally, when a contractor is under * contract to be sold to a foreign owner, or the contractor becomes aware of * negotiations for the sale or transfer of securities to a foreign interest, * such contract of sale or transfer shall be reported by letter. * Reports made pursuant to the foregoing are presumptively proprietary and will be protected from unauthorized disclosure and handled on a strict need-to-know basis. When such reports are submitted in confidence, and so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold them from public disclosure. In cases where the contractor considers the information to be particularly sensitive or delicate and wishes to further restrict dissemination, the foregoing report may be appropriately marked and submitted to the Director, DIS, ATTN: Deputy Director (Industrial Security), 1900 Half Street, S.W., Washington, D.C. 20324-1700.

12/ When the facility or contractor is located on a UA installation, and the Commander or Head of that installation is performing certain prescribed functions of a CSO, the original copy of the report shall be furnished to the Commander or Head of the installation with an information copy of the report furnished to the CSO.

(5) Change in Closed or Restricted Areas, Vaults, and Strongrooms. The contractor shall submit a report of any change in the extent or location of closed areas, restricted areas, vaults, or strongrooms created under the provisions of section IV and appendices IV and V including the establishment of such areas.

(6) Change in Storage Capability. The contractor shall submit a report of any change in the storage capability that would raise or lower the level of classified information the contractor is able to safeguard. (This provision does not require the contractor to report the acquisition of additional containers approved for storage at the same level as that previously reported to the CSO.)

(7) Employee Information in Compromise Cases. The contractor shall submit a report, on the written request of the CSO, of information concerning any employee working in any of his or her plants, factories, or sites where work for a UA is being performed, when the information is needed in connection with the loss, compromise, or suspected compromise of classified information.

(8) Category of Classified Information. The contractor shall submit a report of the highest classification category of classified material received or generated at the facility. However, when the classification of the material received or generated is no higher than that of the material in possession of the facility during the last inspection or previously reported pursuant to this paragraph since the last inspection, an additional report need not be submitted.

(9) Reserved.

(10) Delay in Shipment. The contractor shall submit a report, in accordance with paragraphs 17c(5)(d) and 17d(3)(d), of the delay in the movement of classified material by commercial carriers of more than 48 hours after the expected time of arrival.

(11) Evidence of Tampering. The contractor shall submit a report, in accordance with paragraph 12e(2), of evidence of tampering with a shipment containing classified material. If the material was received through the U.S. Postal System, the contractor shall also promptly notify the appropriate U.S. Postal Inspector.

(12) Improper Shipment. The contractor shall submit a report when a classified shipment is received by other than an approved method prescribed by paragraph 17.

(13) Badges and Identification Cards. The contractor shall submit a report, in accordance with paragraph 8c, which will inform the CSO of the adoption of a new or revised employee badge or identification card system.

(14) Authorization to Apply Classifications. On request, the contractor shall submit a report, in accordance with paragraph 10f(4), of the number of individuals currently authorized by the contractor to apply a classification to information at each of the following categories: TOP SECRET, SECRET, and CONFIDENTIAL.

(15) Location or Disposition of Classified Material Terminated From Accountability. The contractor shall submit a report, in accordance with paragraph 12h(2), when the whereabouts or disposition of classified material previously terminated from accountability is subsequently determined.

(16) Inability to Safeguard Classified Material. The contractor shall submit a report, by the most expeditious means, of any emergency situation, such as a natural disaster or civil disturbance, which renders the facility incapable of safeguarding all classified material (see paragraph 5w). A report shall also be provided to all contracting officers concerned. This requirement of the DoD does not preclude similar reporting of the incident to appropriate local, state, and federal civil authorities, as the situation warrants.

(17) Foreign Classified Contracts. The contractor shall submit a report of any precontract negotiation or award of a foreign or NATO contract for a foreign firm or government involving either U.S. or foreign classified information which is not placed through a UA.

(18) Receipt of Classified Material Not Related to a Classified Contract, Project, or Program. The contractor shall submit a report of the receipt of any classified material, which is not related to a contract, project, or program and for which no specific safeguarding and disposition instructions have been received; further, if the contractor has been unable to obtain classification guidance or disposition instructions from the government originator, or the government activity releasing the material, the report shall so state. The report should identify the material by source, originator, quantity, subject or title, date, and classification category.

(19) Visits by Designated Country Representatives or Nationals. *
The contractor shall submit a report, as soon as the visit arrangements are *
known, of the intent to host a visit by representatives or nationals of a *
Designated country. The report shall include the name and address of the *
contractor to be visited, the name(s) of the employee(s) who will serve as *
host(s), their clearance status, the name(s) of the visitor(s) and the *
foreign firm or government agency and country represented, and the date and *
purpose of the visit. If access to information which relates to a classified *
contract or project is involved, the report shall include a description *
of the information and any other information concerning the visit which may *
be pertinent. In preparation for the visit, the contractor shall provide a *
defensive security briefing and a counterintelligence awareness briefing to *
personnel hosting the visit and others expected to interface with the *
visitors. Disclosure of unclassified information pertaining to classified *
contracts is governed by the provisions of paragraph 5o. The contractor *
shall include in the report a statement as to whether paragraph 5o is *
applicable or an export license 8/ is required. *

b. For all cleared personnel, the contractor shall submit the following reports immediately to the DISCO, Columbus, Ohio 43216-5006, unless the individual involved is or was required to be cleared in connection with the FCL pursuant to paragraph 22, in which case the report will be submitted to the CSO 11/ 12/.

(1) Adverse Information 13/. Contractors shall submit reports, classified if appropriate, of any information coming to their attention concerning any of their employees who have been cleared or who are in the process of being cleared for access to classified information, which indicate that such access or determination may not be clearly consistent with the national interest. The subsequent discharge of an individual by the contractor who receives this information does not obviate the requirement to submit this report. In addition, if the individual is employed on a UA installation, a copy of such report shall be furnished to the Commander or Head of the UA installation. Furthermore, the contractor will also notify such UA installations of the favorable resolution of the reported information after DISCO so notifies the contractor via letter. This requirement to submit information reports also applies to individuals who have been granted a CONFIDENTIAL clearance by the contractor in accordance with paragraph 24b, cleared temporary help supplier personnel and Type A Consultants utilized by the contractor. This requirement in no way affects the temporary help supplier's responsibility for submission of such reports when adverse information regarding his or her employee is brought to his or her attention. The report shall be on company letterhead or identified by typing the contractor's name and address, and addressed to DISCO, ATTN: Chief, Special Programs Branch. Reports submitted under this paragraph shall include: date of submission; subject's last name, first name and middle name; social security number; date and place of birth; level and date of clearance; home address; facility CAGE where the clearance is held; reporting facility's CAGE; subject's physical worksite; employment status (if terminated, add termination date); the adverse information being reported (if a garnishment,

---

13/ As a general rule, any information that reflects adversely on the integrity or character of the employee, which suggests that his or her ability to safeguard classified information may be impaired, should be reported to DISCO. In turn, DISCO will evaluate the information and decide whether further action is warranted. The following are some examples of the types of information (that is, based on incidents which may occur within or outside the contractor facility), which should be reported to DISCO: criminal activities; bizarre or notoriously disgraceful conduct; treatment for mental or emotional disorders; excessive use of intoxicants; use of illegal, controlled substances such as marijuana, heroin, cocaine, and hashish; and excessive indebtedness or recurring financial difficulties. These examples are not all inclusive, but are intended only to serve as a sample of the types of information which should be reported. Only information which has been confirmed by the contractor as fact need be reported. Reports based on rumor or innuendo should not be made under this paragraph. If there is doubt whether information should be reported, furnish the information to DISCO for evaluation. In two court cases, Becker vs. Philco and Taglia vs. Philco (389 U.S. 979), the U.S. Court of Appeals for the 4th Circuit decided on February 6, 1967, that a contractor is not liable for defamation of an employee because of reports made to the government pursuant to the requirements of the ISM. Culpability for a security violation, regardless of whether classified information is found to have been compromised, is a matter which is presumptively reportable pursuant to this paragraph.

please list date of garnishment, court, amount and complainant, or attach a copy of the garnishment order); the name and telephone number, including extension, of the individual to contact for further information regarding the matter; and the signature, typed name and title of the individual submitting the report. Additionally, if appropriate, the report shall include the administrative actions taken against the individual as required by paragraph 5aj. * *

(2) Change in Employee's Status. The contractor shall report (i) the death; (ii) the change in name; (iii) the termination of employment; (iv) a layoff or leave of absence for an indefinite period, or for a prescribed period in excess of 120 days; and (v) residence or assignment outside the U.S., Puerto Rico, Guam, or the Virgin Islands for a period in excess of 90 consecutive days during any 12-month period of those employees who are cleared, or who are in the process of being cleared. Such changes shall be reported by submission of a DISCO Form 562, "Personnel Security Clearance Change Notification."

(3) Official Investigation. Contractors shall submit reports, on the written request of DISCO, of information concerning any employees working in any of their plants, factories, or sites where work for a UA is being performed, when the information is needed in connection with an official investigation.

(4) Relationships in Designated Countries. The contractor shall submit a report, in accordance with paragraph 5v, of the establishment of a relationship between a cleared employee, or one who is in the process of being cleared by the DoD, and a citizen or resident of a Designated country.

(5) Representative of a Foreign Interest. The contractor shall submit a report of any cleared employee (including those in the process of being cleared by the DoD), except those covered by paragraph 6a(4), who becomes an RFI, as defined in paragraph 3bw, or whose status as an RFI changes in a manner that would make him or her ineligible for a PCL pursuant to paragraph 20k.

(6) Changed Intentions and Foreign Residence or Assignment of Immigrant Aliens. The contractor shall submit a report of: (i) residence or the assignment of a cleared immigrant alien outside the U.S. -- such individuals on visits of 90 consecutive days or less to foreign areas are not considered to be assigned outside the U.S., or (ii) a change in the intention of a cleared immigrant alien to reside permanently in the U.S. An immigrant alien's change of intent to reside permanently in the U.S., and residence or assignment of an immigrant alien outside the U.S., negates the basis (see paragraph 31.1) on which the LAA was issued, and the LAA will be administratively terminated without prejudice by DISCO on receipt of contractor notification. Except in connection with visits of 90 consecutive days or less, immigrant aliens may not be authorized access to classified information when visiting outside the U.S. Visits in excess of 90 consecutive days duration, shall invalidate any existing clearance.

(7) Citizenship by Naturalization. The contractor shall submit a report of a cleared immigrant alien who becomes a citizen through naturalization. This report will be made by the "Personnel Security Clearance Change Notification" (DISCO Form 562), setting forth in the "Remarks" block:

(i) city, county, and state where naturalized; (ii) date naturalized; (iii) court; and (iv) certificate number. On receipt of such a report, DISCO will issue a new LOC (DISCO Form 560).

(8) Reserved.

(9) Personal Exchange, Travel or Attendance at Meeting. The contractor shall submit a report of the following: (i) any personal exchange 10/ with nationals or representatives of Designated countries, (ii) completion of travel to or through a Designated country, (iii) or attendance at an international meeting where Designated country representatives participated or attended. The report shall include the employee's full name, clearance status, date and place of birth, a brief description of the projects, including the category of classified information, to which he or she had access during the past 2 years. In the case of a personal exchange, the report shall include the name(s) of the national or representative, the Designated country involved, and the circumstances of the exchange to include an indication if it will be continuing. Foreign travel reports shall include the countries visited, the dates of the travel, and the employee's statement of the purpose and objective of the travel. In the case of attendance at a meeting, the report shall identify the meeting attended to include dates and location. Any of the above reports shall include, if appropriate, a narrative statement of the circumstances surrounding all efforts by a national or representative of a Designated country to obtain information from or to compromise the employee or to establish a continuing relationship with the employee. For a cleared employee assigned overseas, a copy of the report shall be submitted to OISI.

(10) Employees Desiring Not to Perform on Classified Work or Accept Security Responsibility or Requests to Terminate Clearance or Clearance Processing. The contractor shall submit a report on notification by an employee that he or she no longer wishes to be processed for a PCL, pursuant to paragraph 26, or to continue an existing PCL.

(11) Classified Information Nondisclosure Agreement, SF 312. The contractor shall submit a report in accordance with paragraph 5g, when an employee refuses to execute the SF 312.

c. The contractor shall promptly submit a written report 14/, to the nearest field office of the FBI, classified if appropriate, regarding information coming to his or her attention concerning existing or threatened espionage, sabotage, or subversive activities at any of his or her plants, factories, laboratories, or other sites, at which work for any UA is performed, or at which related material is acquired, stored, fabricated, or manufactured, or is in process of research or development.

14/ If time is of the essence and the initial report is made via phone to the FBI, it must be followed in writing, regardless of disposition made of the report by the FBI.

7. Loss, Compromise, or Suspected Compromise of Classified Information [15].

a. The contractor shall establish a procedure to ensure that each loss, compromise, or suspected compromise of classified information and each failure to comply with a requirement of this manual is immediately reported to the FSO. Classified material which is out of the control of its custodian or which cannot be located shall be presumed to be lost until an investigation determines otherwise.

b. The contractor shall establish such procedures as are necessary to ensure that any employee discovering the loss, compromise, or suspected compromise of classified information outside a facility promptly reports such a fact to:

(1) the nearest office of the FBI, and furnishes sufficient information to assist in identification of the information -- if the loss, compromise, or suspected compromise occurs outside the U.S., the nearest U.S. authorities shall be notified in lieu of the FBI; and

(2) the FSO, by the fastest means of communication, who will then comply with paragraph c below.

c. Immediately on receipt of a report, in accordance with paragraphs a or b above, the contractor shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise, suspected compromise, or failure to comply with a requirement of this manual. To obtain the required information, it may be necessary to check records, review the SPP, examine material evidence, and interview persons having direct knowledge of the facts of an incident. The preliminary inquiry should include the following:

(1) What is alleged to have happened, where, and when did the violation occur?

(2) Who reported the violation, to whom, and when?

(3) What classified information was involved? (Attach a list of the classified material, if appropriate.)

(4) What was the classification of the information involved?

(5) Who are the originators of the information involved? Identify the procurement activity (PCO & ACO) and prime contract number.

(6) When, for how long, and under what circumstances was classified information vulnerable to unauthorized disclosure? Determine identity of unauthorized persons likely to have had access to the classified information.

---

[15] In addition to the reporting requirements outlined in this paragraph the contractor shall promptly notify the appropriate U.S. Postal Inspector of any loss, compromise or suspected compromise of classified information that occurred while such information was in the U.S. Postal System.

(7) What actions were taken to secure the classified information and/or limit the damage before the inquiry began, and when and by whom were they taken (inventories, securing of material, changing of combinations, and so forth)?

(8) Is any classified material lost or unaccounted for? (In the event of a loss, a thorough search shall be conducted for the classified material.)

d. If the contractor's preliminary inquiry prescribed in paragraph c above confirms: (i) that a loss, compromise, or suspected compromise of any classified information occurred; or (ii) that a violation of a requirement of this manual involving TOP SECRET, COMSEC, special access information, or RESTRICTED DATA occurred, the contractor shall immediately submit a report of the incident to the CSO in accordance with paragraph 6a(2) or 6a(3), as appropriate, and conduct a complete investigation of the incident unless otherwise notified by the CSO. The initial report shall include as much of the information specified in c(1) through c(8) above, as possible. Submission of the initial report shall not be deferred pending completion of the contractor's investigation. In those instances when the contractor's preliminary inquiry does not confirm a violation that requires a report to the CSO, the contractor shall make a written record of the results of the inquiry that includes the specific reasons for reaching the conclusion that compromise did not occur. This record will be kept available for review during the next government security inspection by the CSO. When individual culpability is established, a report shall be submitted in accordance with 6b(1).

e. On completion of the investigation prescribed in paragraph d above, a final report shall be submitted to the CSO referencing the preceding preliminary report, and containing the following:

(1) any of the information required by paragraphs c(1) through c(8) above that was not included in the initial report;

(2) the name, position, social security number, date and place of birth and date of PCL or LAA of the individual(s) who was primarily responsible for the incident; including a record of prior loss, compromise, suspected compromise, or failure to comply with the requirements of this manual for which the individual had been determined responsible; * * * * *

(3) a statement as to the corrective action taken to preclude a recurrence of similar incidents and the disciplinary action taken against the responsible individual(s), if any; and

(4) specific reasons for reaching the conclusion that: (i) loss or compromise occurred, (ii) compromise is suspected, (iii) the probability of compromise is considered remote, or (iv) compromise did not occur.

8. Badges and Identification Cards.

a. Employee Badges and/or Identification Cards. Provided the contractor deems it necessary, he or she may use color or symbol coded identification badges or cards, or a combination of the two to assist in identifying the level of security clearance of the holder and/or to indicate that the holder is authorized to enter specified closed or restricted areas. However, coded badges and cards shall be considered only as an aid in determining the current level of PCL/LAA of the holder or the closed or restricted areas to which the holder may have access. Release of classified information or entrance to a closed or restricted area, on the sole basis of an identification badge or card, is not authorized. Further, whenever a combination of badges or cards is used, both must bear correlating data such as the same registration number or the name of the holder. If identification cards or badges are used for such purposes, the following shall apply.

(1) The minimum identifying information to be shown on an employee's identification badge or card shall be the name and photograph of the holder. Other descriptive information to identify the authorized holder may be included on badges and/or cards at the option of the contractor.

(2) The words TOP SECRET, SECRET, or CONFIDENTIAL, or abbreviations thereof, shall not appear on the badges or identification cards.

(3) For entry into a closed or restricted area or access to classified information the contractor must establish some additional method for verifying clearance and need-to-know to be used in collaboration with the identification badge or card system. To the maximum extent possible, personal recognition should be the basis for ensuring that the holder of the badge or identification card has an appropriate PCL or LAA and need-to-know. When personal recognition is not possible, the individual responsible for the security of the closed or restricted area or holder of the classified information shall verify the identity of the individual and determine whether the individual has the appropriate PCL or LAA and need-to-know. This can be accomplished in a number of ways, including access lists, verification of clearance status through the office of the FSO, and the need-to-know through the prospective recipient's supervisor. Where cipher or similar locks are used in closed or restricted areas, the individual's knowledge of the cipher-lock combination, coupled with his or her badge, would establish the individual's authority for entry into the area.

(4) The make-up and construction of badges and identification cards shall be designed to minimize the possibility of tampering or unauthorized use.

(5) Badges and identification cards coded to indicate the level of security clearance or access to closed or restricted areas, shall be rigidly controlled and accounted for by the contractor by use of a numbering system. Such controls shall apply equally to permanent and temporary cards and badges. Badges and identification cards shall be promptly recovered or, when appropriate, recoded whenever an employee's requirement for entry to a closed or restricted area no longer exists due to an internal transfer, termination of employment, revocation of PCL, or for other appropriate reasons.

(6) Coded badges and cards shall be considered only as an aid in determining the current level of PCL or LAA of the holder or the areas to which the holder may have access. The clearance status of a person who holds such a badge or identification card shall be verified when there is doubt as to the validity of the badge or card.

(7) An employee badge and/or identification card may be issued to persons referred to in paragraphs 37h and 41a.

b. Visitor Badges. A badge of such design as the contractor considers suitable may be issued to assist in identifying visitors who are authorized to be present in closed or restricted areas. Visitors' badges, except for those issued in accordance with paragraph a(7) above, shall not be used to indicate a visitor's PCL or LAA status. Visitors' badges shall be recovered at the conclusion of their visit, and they shall be rigidly controlled and accounted for by the contractor.

c. Reporting. The procedure for use of badges or identification cards, as authorized in paragraphs a and b above, shall be incorporated in the SPP. In addition, the adoption of a new employee badge or identification card system or any change in an existing badge or identification card system shall be reported to the CSO in accordance with paragraph 6a(13).

d. Use on User Agency Installations. The use of badges or identification cards to indicate the level of PCL or LAA of individuals performing duties within a UA installation shall be subject to regulations which apply to the installation.

9. DoD Sponsorship of Meetings. Meetings described in paragraph 5q(3) which serve a government purpose and at which adequate security measures have been provided for in advance may be sponsored. As used herein, sponsorship shall refer only to sponsorship for security purposes which shall require a DoD Component to undertake all security responsibility and administration of the meeting. However, in the case of a meeting as described in paragraph 5q(3), the DoD Component having primary responsibility for the information involved may designate a cleared DoD contractor to undertake overall responsibility for security and administration.

a. Requests for Sponsorship. Contractors desiring to conduct meetings requiring DoD sponsorship shall submit their requests to the DoD activity having principal interest in the subject matter of each meeting. Only one activity may sponsor a meeting on behalf of the DoD. Therefore, a request shall be sent only to one DoD activity at a time. If that activity declines to accept sponsorship, or if it is appropriate to change the sponsoring agency, the request may be sent to another DoD activity having a principal interest in the subject matter of the meeting. Such requests shall include the details concerning all prior requests. Approval and sponsorship by the DoD will normally be granted only for a meeting conducted by a cleared DoD contractor. However, a meeting conducted by an association, contractor, institute, or society, whose membership is comprised primarily of cleared DoD contractors, contractor employees, or DoD personnel, may be sponsored for security purposes by the DoD, provided that a cleared contractor is designated and accepts overall security responsibility for the meeting on behalf of the association, society, or group. The request shall explain how the interests of national defense will be served by disclosing classified information at the meeting, and why the use of conventional channels for release of the information will not accomplish the purpose of those interests. The request shall also include a list of any foreign nationals or RFI's (including the names of the individuals, firms, or governments) whose attendance at the meeting is required.

b. Attendance of Foreign Nationals or RFI 16/. No invitation, written or oral, shall be tendered to a foreign national, or to an RFI, to attend any session of a meeting sponsored by a DoD activity, until approval or his or her attendance has been received from the sponsoring activity. If the attendance of a foreign national or RFI is required, a written request in advance of the meeting shall be submitted and shall include:

(1) identification of the foreign national or RFI by name, nationality, and government, for the individual or firm represented;

(2) sessions or subject matter for which access authorization is desired (nationals or representatives of Designated countries shall be excluded without exception, from attendance at any classified session); and

(3) subject titles of scientific, technical, and other papers scheduled for presentation by any foreign national or representative of a foreign national or RFI.

c. Location of Meetings. The sponsoring activity is responsible for evaluating and approving the location proposed for the meeting.

(1) Meetings at which TOP SECRET or SECRET information is to be disclosed shall be held only at a U.S. Government installation or at an appropriately cleared facility of a contractor, which has adequate means for safeguarding classified presentations. Under this criteria, the proposed site would have to be located within the physical boundaries of a cleared facility. An auditorium, assembly hall, or gymnasium which is used primarily for campus activities and public gatherings will not be approved for a classified meeting at which TOP SECRET or SECRET information would be disclosed, even though it is located on the campus of a college or university, portions of which are a cleared facility.

(2) Meetings at which information classified no higher than CONFIDENTIAL is to be disclosed shall normally be held at a U.S. Government installation or a cleared facility. However, if suitable facilities are not available at a U.S. Government installation or contractor facility, the use of other locations may be approved, provided adequate security can be maintained. Contractor requests to use a location other than a U.S. Government installation or contractor facility shall include:

(a) a justification of the proposed location;

(b) an explanation why a U.S. Government installation or cleared facility cannot be used; and

(c) an explanation why separate classified and unclassified sessions cannot be scheduled, thereby permitting the use of a U.S. Government installation or a cleared facility for the classified portions of the meeting.

16/ Foreign nationals granted LAA's, and RFI's cleared for access to classified information under the DoD Industrial Security Program, are not subject to the limitation of paragraph 9b. However, persons granted LAA's clearances are subject to the access limitations prescribed in paragraph 31.3.

d. Security Procedures. When sponsorship of a meeting has been accepted by a DoD activity, the contractor shall develop the security measures and procedures to be used, and obtain the sponsoring activity's approval thereof. The security measures shall include adequate arrangements for the following:

(1) Security measures shall include strictly limiting attendance at classified meetings to those persons whose presence is necessary in the interest of national defense and who are otherwise eligible. This shall include measures for the following:

(a) Security measures shall include determining and ensuring that all persons selected and approved to attend classified sessions have been granted a PCL for access to classified information equal to or higher than the category of information to be disclosed, and have duties in connection with a classified contract or program that requires such access in promoting the interests of national defense. For contractor personnel, the certification of PCL and need-to-know shall be accomplished as provided in paragraph f below.

(b) Security measures shall include review and approval by the sponsoring activity of all announcements and invitations related to the meetings and lists of attendees pertaining thereto. Announcements and invitations shall be unclassified, and shall include the name of the sponsoring activity and the date of the approval.

1 Notices and announcements of meetings, whether classified, unclassified, or mixed, and not amounting to invitations to attend, may be published publicly, provided classified information is not included in such notices or announcements.

2 In the case of classified meetings, invitations to attend (whether on an individual or class basis) shall not be sent to a person known to be a national from or a representative of a Designated country.

3 In the case of mixed meetings, that is, those having both classified and unclassified sessions, the restrictions as to invitations to persons known to be nationals from, or representatives of, a Designated country to attend are applicable to the classified session. As to the unclassified session, such notice or invitation to attend shall not be sent to persons known to be nationals from, or representatives of, a Designated country, unless and until specific authorization, on an individual name basis, has been made in advance by the Secretary or Head of the DoD Component.

(2) Security measures shall include safeguarding and controlling the distribution of notes, minutes, summaries, recordings, proceedings, and reports on the classified portions of the meeting. Such material shall normally be sent only to those approved for attendance at the classified sessions. However, the sponsoring activity may also authorize distribution to others who are determined to be eligible for, and require access to, the classified information involved. In any event, the material shall only be sent to a U.S. Government activity or cleared contractor facility and marked for the attention of the intended recipient, as provided for in paragraph 17k.

(3) Security measures shall include notifying each person who presents or discloses classified information at the meeting of the security

limitations on disclosures for such reasons as the level of clearance or need-to-know of members of the audience or other limitations established by the U.S. Government.

(4) Security measures shall include ensuring the physical security of the meeting site and the area used for classified sessions or displays. This shall include provisions for guards, entrance controls, personnel identification, storage facilities, and adequate security against unauthorized access to, or illicit acquisition of, the classified information.

(5) Security measures shall include ensuring that attendance at a meeting or session at which classified information is to be disclosed is limited to persons whose names appear on an approved access list, and then only on proper identification.

(6) Security measures shall include submitting the minutes, summaries, recordings, proceedings, and reports of the meeting to the sponsoring activity for security review and for approval of the proposed distribution.

(7) Security measures shall include ensuring that individuals making oral presentations at meetings provide classification guidance sufficient to enable attendees to identify what information is classified or unclassified and, if classified, at what category or categories of classification.

e. Request for Disclosure Authority. A contractor desiring to disclose classified information at a meeting as provided in paragraph 5q(3) or 5q(4) shall:

(1) obtain prior written authorization for each proposed disclosure of classified information from the contracting officer having jurisdiction over the information involved -- if authorization for foreign nationals to attend the meeting has been requested from the sponsor, that fact shall be stated in the request for disclosure authority;

(2) furnish a copy of the disclosure authorization to the U.S. Government activity conducting or sponsoring the meeting; and

(3) furnish a written copy of the presentation, as made, to the contracting officer and to the conducting or sponsoring activity, if they are not one and the same.

f. Requests to Attend Classified Meetings. A contractor desiring to have an employee attend a classified meeting shall:

(1) certify to the PCL status and need-to-know of the employee who will attend the classified meeting, and

(2) forward the application or request to attend the meeting, together with the necessary justification (see paragraph d(1)(a) above), to the contracting officer for the classified contract under which access is being justified, requesting that it be forwarded to the sponsoring activity. However, where access is being justified under a UA program, rather than a contract, the request shall be forwarded to the official of the UA activity who is monitoring the contractor's participation in the program.

Section II. HANDLING OF CLASSIFIED INFORMATION

10. Classification.

a. The security classification (TOP SECRET, SECRET, or CONFIDENTIAL) to be applied to information involved in a UA classified contract will be supplied to the contractor by the contracting officer or the designated representative of the UA concerned. The DD Form 254 is the basic document used to convey the classification, regrading, downgrading, and declassification specifications for a classified contract. The DD Form 254, with any necessary attachments or supplements, as appropriate (hereinafter referred to only as the DD Form 254), provides the guidance to be used for this purpose. The DD Form 254 identifies the specific items of classified information involved in the contract that require security classification protection. Contractors shall, to the extent practicable, advise and assist in the development of the original DD Form 254 and the security classification guide in order that their technical expertise may be utilized. By so doing, contractors are also in a better position to anticipate the security costs and requirements under the contract and may organize attendant procedural aspects and physical plant layout accordingly. It is the contractor's responsibility to understand and apply all aspects of the classification guidance. Contractors may submit recommended changes for a revised DD Form 254 if they encounter difficulty in applying or interpreting the DD Form 254 during any phase of the contract. Classification guidance is, notwithstanding the contractor's input, the exclusive responsibility of the User Agency, and the final determination of the appropriate classification rests with that agency. The DD Form 254 is a contractual specification necessary for performance on a classified contract. If a classified contract is received without a DD Form 254, the contractor shall advise the UA concerned. The CSO may be requested to provide assistance, if desired.

b. An original DD Form 254, which sets forth the classification specifications or cites the classification guidance in item 15, is provided to the contractor by the UA with an RFP, RFQ, IFB, or other solicitation and with the award of a contract which will necessitate access to classified information. A revised DD Form 254 will be issued at any time a change or additional classification guidance is necessary. The UA reviews the existing classification specifications periodically during the contract and at least once every 2 years. When the biennial review establishes that no change is necessary in the existing guidance, the prime contractor is advised in writing. A final DD Form 254 is issued on final delivery of goods or services or on termination of the contract when authority is granted under paragraph 5m for the contractor to retain classified material originated by the UA or generated by the contractor in the performance of the contract, or when all classified material, for which retention authority would be required, is ordered immediately declassified. A final DD Form 254 is not issued, however, when authority is granted under paragraph 5m for the contractor to retain only reference material (see paragraph 3bt).

c. At the end of a retention period authorized under paragraph 5m, if the contractor requests an extension of the retention period, the UA will conduct a review to ensure that the contractor has a continued requirement for possessing the classified material and to revise the existing classification specifications as necessary to cover the classified material for which an extension of retention authority is authorized.

d. The application of a security classification to information developed by the contractor shall be based on: (i) the classification guidance furnished by the contracting officer of the UA, in accordance with paragraph a above, or (ii) the contractor's knowledge that such information is in substance the same as, or would reveal, other information known to be currently classified. Material developed by the contractor containing classified information, or from which classified information could be obtained, shall be marked in the manner prescribed in paragraph 11.

e. Contractors who have reason to believe that information is classified improperly or unnecessarily, or believe that current security considerations justify downgrading to a lower classification or upgrading to a higher classification, or believe that the security classification guidance provided is improper or inadequate, are required to discuss such problems with the UA involved with a view to bring about correction. If a solution is not forthcoming, and the contractor believes that corrective action is still required, a formal challenge shall be made to the UA that originally classified the information. Such challenges shall include a description sufficient to identify the problem, the reasons why the contractor believes that corrective action is required, and any recommendations for appropriate corrective action. In any case, the information in question shall be safeguarded as required by this manual for its assigned or proposed level of classification, whichever is higher, until action is completed. If no answer is received within 45 days, the CSO may be requested to provide assistance in obtaining a response. The fact that a contractor has initiated such a challenge shall not in any way result in or serve as a basis for any adverse action by the UA involved.

f. The contractor shall establish a procedure to ensure the following:

(1) In the case of a document, and except as specified in paragraph (3) below, the manager or supervisor, whose signature or other form of approval is required before the document may be issued, transmitted, or referred outside of the facility, determines the necessity, currency, and accuracy of the classification applied to that document.

(2) In the case of material other than a document, and except as specified in paragraph (3) below, the manager or supervisor in charge at the operational level where the material is being produced or assembled determines the necessity, currency, and accuracy of the classification applied to that material.

(3) In those situations involving the copying or extracting of classified information from another document, or involving the reproduction or translation of a whole classified document, the individual responsible for such copying, extracting, reproduction, or translation marks the new document or copy with the same classification as that applied to the information or document from which the new document or copy was prepared. However, if the contractor believes the classification marking is improper in any respect, such marking shall be in accordance with a final disposition of the contractor's action under paragraph 10e.

(4) Employees responsible for the currency, necessity, and accuracy of the classification applied to information, under paragraphs (1) and (2) above, are held to a minimum number consistent with operational requirements. The number of such employees shall be reported to the CSO on request in accordance with paragraph 6a(14).

(5) Questions on the currency of the classification of reference material are referred as indicated in paragraph 60i.

g. Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a UA contract or program, the following rules shall apply:

(1) If information is included in the proposal or other material which the contractor identifies as already being classified, the proposal or other material shall be marked with the appropriate classification in accordance with paragraph 11.

(2) If the case does not fall within paragraph (1) above, and the contractor believes that the proposal or other material contains information which may or should be safeguarded, the contractor is requested to protect the information as though classified at the appropriate level, until an advisory classification opinion is obtained from a UA which has an interest in the subject matter. In any such case, the following protective marking, or a similar marking which clearly conveys the same meaning, will be used:

Classification determination pending.
Protect as though classified
(CONFIDENTIAL, SECRET, or TOP SECRET)

This marking shall appear conspicuously at least once on the material, but it is not necessary to mark the material further in accordance with paragraph 11 until the advisory classification opinion is received. In addition, if applicable, contractors are not precluded from designating such information as company private or proprietary information.

(a) Pending determination by the UA, the following precautionary measures should be taken in regard to safeguarding such information:

1 Access to the information should be limited to the minimum number of personnel practical.

2 Persons selected to have access to the information should be limited to U.S. citizens who are known to be trustworthy. They should be advised of the importance of the information. *
*
*

3 When not in use, documents containing the information should be stored in a secure container.

4 In forwarding the information between persons or locations, a secure method of transmission should be used.

5 Reproduction of the information should be kept to a minimum.

(b) It is the policy of the U.S. Government not to classify information over which it has no jurisdiction. The proposal or other material shall not be classified by the UA: (i) unless it incorporates classified information to which the contractor was given prior access, or (ii) unless the government first acquires a proprietary interest in the information.

h. The contractor shall provide security classification guidance to employees performing in a sales or technical capacity and under a classified contract outside of the U.S.

i. The fact that information currently classified by a UA has been disseminated by a public medium of communication does not automatically mean that it has been declassified. Classification shall be continued until advised to the contrary by the UA. Questions as to the propriety of continued classification in these cases should be brought to the immediate attention of the contracting officer.

11. Marking.

a. General. Classification designation by physical marking, notation, or other means serves to warn and to inform the holder what degree of protection against unauthorized disclosure is required for that information or material. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked in such a manner that it is clear to the holder what level of classification is assigned to the information or material, exactly what portions of the information or material contain or reveal classified information, how long the protection is required, and any other additional markings required for protection of the information or material.

b. Marking Requirements for Information and Material. The markings shown in paragraphs (1) through (8) below are required for all classified information, regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be marked easily with the appropriate markings. Marking other material, such as equipments, ADP media, and slides, will be more difficult due to size or other physical characteristics. Since the purpose of the markings is to warn the holder that the information requires special protection, it is necessary that all classified material be marked with the appropriate markings to the fullest extent possible to ensure that it is afforded the necessary safeguards.

(1) Identification Markings. All classified material shall be marked to show: (i) the name and address of the facility responsible for its preparation, and (ii) the date of preparation. These markings are required on the face of all classified documents.

(2) Overall Markings. The overall classification of a document, or any copy or reproduction thereof, shall be conspicuously marked or stamped at the top and bottom, on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover

(if any). If the document does not have a back cover, the outside of the back or last page, which may serve as a cover, may also be marked at the top and bottom with the overall classification of the document. The markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material, other than documents, and on containers of such material, if possible. If marking the material or container is not practical, written notification of the appropriate markings shall be furnished to recipients. Copies of documents shall include the appropriate markings on the documents themselves.

(3) Page Markings. Interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the portions on the page are UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency and so that the particular information to which classification is assigned is adequately identified, in accordance with paragraph b(5) below. In any case, the classification marking of a page shall not supersede a lower level of classification indicated by a portion marking applicable to information on that page.

(4) Component Markings. The major components of complex documents are likely to be used separately. In such instances, each major component shall be marked as a separate document utilizing the classification marking requirements of this manual. Examples include: (i) each annex, appendix, or similar component of a plan, program, or project description; (ii) attachments and appendices to a letter; and (iii) each major part of a report. If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation "UNCLASSIFIED" and a statement included, such as, "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method of marking is used, no further markings are required on the unclassified major component.

(5) Portion Markings. Each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification, or that such portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. For the purpose of applying these markings, a portion or paragraph shall be considered a distinct section or subdivision of a chapter, letter, or document dealing with a particular point or idea which begins on a new line and is often indented. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking portions, the parenthetical symbols "(TS)" for TOP SECRET, "(S)" for SECRET, "(C)" for CONFIDENTIAL, and "(U)" for UNCLASSIFIED shall be used. When appropriate, the symbols "RD" for RESTRICTED DATA and "FRD" for FORMERLY RESTRICTED DATA shall be added, for example, "(S-RD)" or "(C-FRD)." In addition, portions that contain Critical Nuclear Weapon Design Information (CNWDI) will be marked "(N)" following the classification, for example, "(TS-RD)(N)."

(a) Portions of U.S. documents containing foreign government information shall be marked to reflect the country or international organizations of governments of origin as well as the appropriate classification, (for example, "(NATO-S)" or "(U.K.-C)," or "(NATO-R)" for NATO-RESTRICTED), except where such markings would reveal that the information is foreign government information, when that fact must be concealed, or if a confidential source or relationship not otherwise evident in the document is revealed. Where a UA determines that this information would be revealed, the classification specifications and source documents furnished to contractors will not bear this information, and in these cases contractors will not identify the foreign governments in any classified material generated. See paragraph (8)e below for other marking requirements for foreign government information.

(b) When illustrations, photographs, figures, graphs, drawings, charts, or similar portions are contained in classified documents they shall be marked clearly to show their classified or unclassified status. In this instance, such markings shall not be abbreviated and shall be prominent and placed within or contiguous (touching or near) to such a portion. Captions of such portions shall be marked on the basis of their content alone by placing the symbol "(TS)," "(S)," "(C)," or "(U)" immediately preceding the caption.

(c) If, in an exceptional situation, parenthetical marking in the portions is determined to be impractical, the classified document shall contain a description sufficient to identify the exact information that is classified and the classification level(s) assigned to it. For example, each portion of a document need not be separately marked if all portions are classified at the same level, provided a full explanation is included in the document.

(d) When elements of information in one portion or paragraph require different classifications, but segregation into separate portions or paragraphs would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

(6) Subject and Title Markings. Subjects and titles of documents shall be selected, if possible, so as not to require classification. A classified subject or title shall be marked with the appropriate symbol (TS), (S), or (C) placed immediately following and to the right of the item. An unclassified subject or title shall be marked with a (U) placed immediately following and to the right of the item. When applicable, other appropriate symbols, for example, "(RD)," "(FRD)," "(N)," or "(NATO)" shall be added.

(7) Downgrading/Declassification and "Classified by" Markings. Procedures for marking downgrading and declassification instructions, and for completion of the "Classified by" line are prescribed in appendix II. These markings shall be placed either on the cover, first page, title page, or in a similarly prominent position on classified documents.

(8) Additional Markings. In addition to the markings specified above, classified material shall be marked, if applicable, with one or more of the notations prescribed below, or other markings specified by a UA. The

appropriate notation shall be printed, stamped, typed, or otherwise affixed conspicuously at least once on classified material possessed 1/, prepared, or reproduced by the contractor. In addition, when a copy, extract, or paraphrase of a document contains classified information, or when a page, chapter, or other component is separated from such a document, the extract or component shall also be conspicuously marked at least once with the appropriate notation. In the case of documents, these warning notices shall be conspicuously marked on the outside of the front cover (if any) or on the first page if there is no front cover. When display of warning notices on other materials is not feasible, the warnings shall be included in the written notification provided to recipients.

(a) RESTRICTED DATA Notation. The following notation shall be affixed on all material which contains "RESTRICTED DATA":

RESTRICTED DATA
This material contains RESTRICTED DATA as defined
in the Atomic Energy Act of 1954. Unauthorized disclosure
subject to administrative and criminal sanctions.

(b) FORMERLY RESTRICTED DATA Notation. Except when the "RESTRICTED DATA" notation is used, all material containing information in the "FORMERLY RESTRICTED DATA" category shall be marked with the following notation:

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative
and criminal sanctions. Handle as RESTRICTED DATA in foreign dissemination.
Section 144 b, Atomic Energy Act 1954.

(c) INTELLIGENCE SOURCES OR METHODS Notation. Classified information or material involving intelligence sources or methods and subject to specific dissemination controls shall be marked with the following warning notice 2/:

WARNING NOTICE
INTELLIGENCE SOURCES OR
METHODS INVOLVED

(d) DISSEMINATION AND REPRODUCTION NOTICES. From time to time certain UA's may promulgate certain classified information, which the government agency originating the material has determined should be subject to

---

1/ Classified material that is already marked with officially prescribed additional warning notices that convey in substance the same meanings as those prescribed in paragraph b(8) need not be re-marked.

2/ Existing stamps and preprinted labels containing the caveat, "Warning Notice -- Intelligence Sources and Methods Involved," may be used until a replacement stamp is obtained or the supply of labels is exhausted.

special dissemination or reproduction limitations or both. Statements substantially as follows will be included on the front cover of such documents:

REPRODUCTION REQUIRES APPROVAL OF
ORIGINATOR OR HIGHER GOVERNMENT AUTHORITY.

(Reproduction of all portions of the information contained in such documents is absolutely prohibited without the permission of the originating office or higher government authority.)

FURTHER DISSEMINATION ONLY AS
AUTHORIZED BY CONTRACTING
OFFICER

(Further dissemination within the receiving contractor facility is restricted to persons authorized by the addressee. Dissemination outside the facility is prohibited without the permission of the contracting officer.)

(e) FOREIGN GOVERNMENT INFORMATION. This marking is used on U.S. documents containing "FOREIGN GOVERNMENT INFORMATION" to ensure that such information is not declassified prematurely or made accessible to nationals of a third country without the consent of the originator.

(f) THIS DOCUMENT CONTAINS NATO INFORMATION. This marking is used on U.S. documents which contain extracts from NATO documents to ensure that such information is not declassified or made accessible to nationals of non-NATO countries without NATO approval.

c. Marking Specific Types of Material. The following procedures for marking specific types of material are not all inclusive. Due to the many variations that may occur in the preparation of classified materials, every possible marking situation cannot be addressed. These procedures are for marking various types of material, which are most often encountered by contractors, and may be varied to accommodate the physical characteristics of the material and organizational and operational requirements.

(1) Artwork. Original artwork shall have the overall security classification stamped or conspicuously marked in the top and bottom margins of the mounting board and on all overlays and cover sheets. Other markings specified in paragraphs b(1) through (8) above also shall be included on such documents, as applicable.

(2) Charts, Maps, Drawings, and Tracings. The appropriate classification markings for the legend, title, or scale block shall be shown in the legend, title, or scale block itself, or in such a manner as to differentiate between the overall classification assigned to the document and any classification assigned to the legend or title itself. The overall classification of the document shall be marked or stamped at the top and bottom of each document. Any identifiable portions of such documents shall be marked in the manner prescribed in paragraph b(5) above, if possible. When the customary method of folding or rolling charts, maps, drawings, or tracings would cover the classification markings, additional classification markings

shall be placed so as to be clearly visible when the document is folded or rolled. Other markings specified in paragraphs b(1) through (8) above also shall be included on such documents, as applicable.

(3) Decks of Automatic Data Processing Punched Cards. When a deck of classified AIS punched cards is handled and controlled as a single document, only the first and last cards of the deck require the overall classification markings as specified in paragraph b(2) above. An additional card shall be added (or the job control card modified) to identify the contents of the deck, and to show the appropriate markings specified in paragraphs b(1) through (8) above. Individual cards removed for separate processing or use, and not immediately returned to the deck, shall be protected to prevent compromise of any classified information contained therein, and shall be individually marked to show the appropriate markings specified in paragraphs b(1) through (8) above. Alternatively, a grouping of cards removed for separate processing or use, and not immediately returned to the deck, may be handled, controlled, and marked as a separate deck of cards.

(4) Continuous Form (fan folded or rolled) Documents Produced by AIS Equipment. When a continuous form document is handled and controlled as a single document, that is, its pages are connected, the following minimum markings are allowable:

(a) Conspicuously mark the overall classification at the top and bottom of the first and last page and on the front and back cover, if any.

(b) Internal pages (those between the first and last page in a continuous form document) do not require any classification markings.

(c) Other appropriate markings as required by paragraph b(1), (5), (6), (7), and (8) above shall be shown on the document and may be applied by the equipment or by other comparable means.

When a continuous form document is broken by removal of a single page(s), each page(s) removed shall be marked with all the appropriate markings specified by paragraphs b(1) through (8) above.

When separate continuous form documents are created as a result of removing a single page(s), or otherwise breaking the continuous form, each document created shall be handled, controlled, and marked as a single document.

(5) Files, Folders, or Groups of Documents. Files, folders, binders, envelopes, and other items, containing classified documents, when not in secure storage, shall be conspicuously marked according to the highest classification of any classified document included therein. Classified document cover sheets may be used for this purpose.

(6) Messages. Electronically transmitted messages (that is, those transmitted via authorized CRYPTOSYSTEMS) shall bear appropriate markings as specified in paragraphs b(1) through (8) above, except as noted herein. The first item of information in the text shall be the overall classification of

the message. The message also shall show the date or event for declassification or the notation "Originating Agency's Determination Required" or "OADR," and downgrading action, if applicable. The "Classified by" line information is not required. Portions shall be marked in the manner required for other documents. When messages are printed by an automated system, all markings may be applied by that system, provided that the classification markings are clearly distinguished from the printed text. (NOTE: The highest level official identified on the message as the sender, or in the absence of such identification, the highest level official at the facility originating the message, is deemed to be the classifier of the message. The originator is responsible for maintaining adequate records to show the source of an assigned derivative classification.)

(7) Microforms. Microforms are copies usually produced on transparent or opaque materials in sizes too small to be read by the unaided eye. Accordingly, the appropriate markings as specified in paragraphs b(1) through (8) above shall be conspicuously marked on the microform medium or its container, so as to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. The markings specified in paragraph b(7) above may be abbreviated. Further markings and handling shall be as appropriate for the particular microform involved. For example, roll film microforms (or roll microfilm employing 16, 35, 70, or 105 mm films) may generally be handled as provided for roll motion picture films, and decks of "aperture cards" may be handled as decks of automatic data processing punched cards. Whenever possible, microfiche, microfilm strips, and microform chips shall be handled in accordance with this paragraph.

(8) Motion Picture Films. Classified motion picture films and video tapes shall be marked at the beginning and end of each reel by titles bearing the appropriate classification and applicable associated markings. Such markings shall be visible when projected. Motion picture film and video tape containers shall bear conspicuous classification, declassification, and if applicable, downgrading markings. Other markings specified in paragraphs b(1) through (8) above shall also be applied, if applicable.

(9) Photographs. Photographs shall be marked in such a manner so that a recipient or viewer will know that information of a specified level of classification is involved. Negatives and positives shall be marked, whenever practical, with the appropriate classification and applicable associated markings. Roll negatives or positives may be so marked at the beginning and end of each strip. Containers for negatives and positives shall be conspicuously marked with the highest level of classification of their contents. Other markings specified in paragraphs b(1) through (8) above shall also be applied, if applicable. All prints and reproductions shall be conspicuously marked with the appropriate markings, as specified in paragraphs b(1) through (8) above, on the face side of the print, if possible. Where such markings cannot be applied to the face side, they may be stamped or marked on the reverse side, or affixed by pressure tape label, stapled strip, or other comparable means. (NOTE: When self-processing film or paper is used

to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected as classified information.)

(10) Recordings. Magnetic, electronic, or sound recordings shall contain a clear statement of the overall classification at the beginning and end of the recording which will provide adequate assurance that any listener or receiver will know that classified information is involved. Containers for recordings shall be conspicuously marked with the appropriate classification and applicable associated markings, as specified in paragraphs b(1) through (8) above.

(11) Removable Automatic Data Processing and Word Processing Storage Media.

(a) External. Removable information storage media and devices, employed with AIS's shall bear external markings clearly indicating the appropriate markings as specified in paragraphs b(1) through (8) above. Included are media and devices that store recorded information in analog or digital form, and are generally mounted or removed by the users or operators. Examples include magnetic tape reels, cartridges, and cassettes; removable disks, disk cartridges, disk packs, and diskettes; paper tape reels; and magnetic cards.

(b) Internal. In addition, AIS's employing such media shall provide for internally recorded security markings to ensure that classified information contained therein, when reproduced or generated, will bear appropriate markings as specified in paragraphs b(1) through (8) above. (Existing AIS's previously approved by the CSO shall provide this internal classification identification where the capability exists for implementation without extensive system modification. Alternately, where extensive system modification would be required for existing systems, an exception may be made by the CSO, provided procedures are established to ensure that users and recipients of the media, or the information therein, are clearly advised as to the appropriate markings for the contents. Requirements for the security of nonremovable AIS storage media and clearance or declassification procedures for various AIS storage media are contained in section XIII.)

(12) Translations. Translations of U.S. classified information into a language other than English shall be marked to show the U.S. as the country of origin, with the appropriate U.S. markings as specified in paragraph b(1) through (8) above, and the foreign language equivalent thereof (see appendix XIV of this manual).

(13) Transmittal Documents. A transmittal document, including endorsements and comments when such are added to the basic communication, shall carry on its face a prominent notation as to the highest classification of information transmitted by it and a legend showing the classification, if any, of the transmittal document, endorsement, or comment standing alone. For example, an unclassified document that transmits as an attachment a classified document shall bear a notation substantially as follows: "Unclassified when Separated from Classified Enclosures."

(14) Transparencies and Slides. Applicable classification markings shall be shown clearly on the image of each transparency or slide, and on its border, holder, or frame. Other applicable markings as specified in paragraphs b(1) through (8) above shall be shown on the border, holder, or frame, if possible, or in the image area, in accompanying documentation, or other written notification. When a set of transparencies or slides is handled and controlled as a single document, only the title slide or transparency requires the other applicable markings. Slide and transparency storage containers shall also be marked with the appropriate markings as specified in paragraph b(1) through (8) above.

(15) Working Papers. Working papers and material such as notes, drafts, and drawings accumulated or created in the preparation of a finished document, shall be dated when created and marked in the same manner as prescribed in paragraphs b(2) and (3) above. The remainder of the markings required by paragraphs b(1) through (8) above need not be affixed to the material, until it is entered into the accountability records in accordance with paragraph 12, made a part of a permanent record, or dispatched outside the facility.

(16) Miscellaneous Material. Unless a requirement exists to retain material such as rejects, typewriter ribbons, carbons, and similar items for a specific purpose, there is no need to mark, stamp, or otherwise indicate that the information is classified. (NOTE: Such material developed in connection with the handling, processing, production, and utilization of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and destruction at the earliest practical moment.)

d. Marking of Regraded Documents and Material. Whenever classified information is downgraded, declassified, or upgraded, the material shall be promptly and conspicuously marked to indicate the change [3].

(1) Automatic Downgrading or Declassification Actions. Holders of classified material may take automatic downgrading or declassification actions,

---

[3] In the interest of providing quick and efficient service on requests for classified documents, DTIC re-marks downgraded or declassified documents to reflect such action only on the front and back covers and the title, first, and back pages. A notice will be affixed by DTIC to the front cover or the title page of such documents indicating that it is the responsibility of the recipient (the contractor who requested the document) to complete the re-marking of the regraded document in accordance with this paragraph. Documents originally marked under the provisions of previous E.O.'s may contain pages which do not bear any classification markings. Before extracting or reproducing the information from these pages, recipients should direct any questions they may have concerning the classification of an individual page, chapter, section, and the like, to the originator of the document.

as specified by the markings on the material, without further authority for the action. All old classification markings shall be canceled and the new markings substituted, whenever practical 4/. In the case of documents, as a minimum, the outside of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any), must reflect the new classification markings, or the designation UNCLASSIFIED. Other material shall be re-marked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material. Old markings shall be canceled, if possible, on the material itself. If not practical, the material may be marked by affixing new decals, tags, stickers, and the like to the material or its container.

(2) Other than Automatic Downgrading or Declassification Actions. When contractors are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be re-marked to indicate the change. All old classification markings shall be canceled and the new markings substituted, whenever practical 4/. In the case of documents, as a minimum, the outside of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any) shall reflect the new classification markings or the designation UNCLASSIFIED. In addition, the material shall be marked to indicate the authority for the action, the date of the action, and the identity of the person or contractor taking the action. Other holders shall be notified if further dissemination has been made by the contractor.

(3) Upgrading Action. When a notice is received to upgrade material to a higher level, for example from CONFIDENTIAL to SECRET, or from UNCLASSIFIED to CONFIDENTIAL, the new markings shall be immediately entered on the material, in accordance with the notice to upgrade, and all the superseded markings should be canceled, if applicable. Other holders shall be notified, if further dissemination of the material has been made by the contractor. If contractor-generated material is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified, the following procedures shall apply:

4/ When the volume of material is such that prompt re-marking of each classified item cannot be accomplished without unduly interfering with operations, the custodian may attach downgrading and declassification notices to the inside of the file drawers or other storage container in lieu of the re-marking otherwise required. Each such notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage container to which it applies. When documents or other material subject to downgrading or declassification are withdrawn from the container solely for transfer to another, or when the container is transferred from one place to another, the transfer may be made without re-marking, if the notice is attached to the new container or remains with each shipment. When the documents or material are withdrawn for use or for transmittal outside the facility, they shall be re-marked in accordance with paragraph d(1) or d(2) above.

(a) Determine that all holders of the material are authorized access to it.

(b) Determine that control of the material has not been lost by the communication. (NOTE: When both these conditions are determined to exist, then promptly notify 5/ all holders of the proper classification and markings applicable to the material. If it is found that control of the material has been lost or that unauthorized personnel have had access to it, a report of the compromise to the CSO under the provisions of paragraph 7d is required.)

e. Marking of Foreign Classified Material. Foreign classified material shall be marked in accordance with instructions received from the foreign contracting authority, the CSO, or the UA. In any case, if the classification and the country of origin are in a language other than English, the appropriate equivalent U.S. classification and the country of origin will be marked on the foreign classified material. Except for the foreign security classification designation RESTRICTED, foreign security classification designations, including those of international organizations of governments, such as NATO, generally parallel U.S. classification designations. A table of equivalent classifications is contained in appendix XIV. Many foreign governments and international organizations, such as NATO, use a fourth security designation identified as RESTRICTED to denote a foreign requirement for security protection of a lesser degree than CONFIDENTIAL. Documents received by contractors that are marked with any of the classification designations listed in the last column of appendix XIV shall be marked RESTRICTED together with the country of origin and protected in all respects in the same manner as U.S. CONFIDENTIAL, except that foreign RESTRICTED material may be stored in locked filing cabinets, desks, or other similarly closed spaces that will prevent access by unauthorized persons.

(1) When foreign government information is incorporated in a contractor-generated document, that document shall be identified in a manner to ensure that such information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. This requirement may be satisfied by marking the face of the document with the notation "FOREIGN GOVERNMENT INFORMATION" or with another marking that otherwise indicates that the information is foreign government information. Portions of documents containing foreign government information

---

5/ In the case of material being upgraded, the contractor's written notice shall not be classified, unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as UNCLASSIFIED, the contractor's written notice shall be classified CONFIDENTIAL, unless the notice contains additional information warranting a higher classification. The notice should cite the applicable DD Form 254 or other classification guide on the "Classified by" line and be marked with a declassification instruction such as, "UNCLASSIFIED WHEN UPGRADING ACTION IS COMPLETED."

shall be marked as specified in paragraph b(5)(a) above. All such documents containing foreign government information shall include on the "Declassify on" line the following notation, "ORIGINATING AGENCY'S DETERMINATION REQUIRED," or "OADR," unless the foreign entity has specified or agreed to a date or event for declassification.

(2) U.S. documents which contain extracts of NATO classified information shall be marked on the face of the document with the following notation: "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION." This notation is required to ensure that NATO information is not declassified or made accessible to nationals of non-NATO countries without NATO approval. Portions of such documents shall be marked "NATO" with the appropriate classification, for example, (NATO-S) or (NATO-C). The "Declassify on" line shall be completed with the notation, "ORIGINATING AGENCY'S DETERMINATION REQUIRED," or "OADR," unless the foreign entity has specified or agreed to a date or event for declassification. The marking "FOREIGN GOVERNMENT INFORMATION" is not required on these documents.

f. Marking Wholly Unclassified Material. Normally, wholly UNCLASSIFIED material will not be marked or stamped "UNCLASSIFIED," unless it is essential to convey to a recipient of such material that: (i) the material has been examined specifically with a view to impose a security classification and has been determined not to require classification, or (ii) the material has been reviewed and has been determined to no longer require classification and it is declassified.

g. Marking Compilations.

(1) Documents. In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document. In this instance, the portions of a document classified in this manner need not be marked.

(2) Portions of a Document. If a classified document contains certain portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on the page, and a statement shall be added to the page, or to the document, to explain the classification of the combination or association to the holder. This method of marking may also be used if classified portions on a page, or within a document, will reveal a higher classification when they are combined or associated than when they are standing alone.

12. Record of Classified Material.

a. Accountability Records. The contractor shall maintain, at one or more control stations, an accountability record of all TOP SECRET and SECRET material, and CRYPTO, regardless of classification. The record shall include all such classified material received or produced by, or in the possession or custody of, the contractor and shall reflect as a minimum: (i) the date of receipt or origin, (ii) the activity from which received or by which originated, (iii) the classification of the material, (iv) a brief, unclassified description of the material and (v) the disposition of the material and the date thereof (that is, destroyed, downgraded to CONFIDENTIAL, declassified, or dispatched outside the facility). These records shall be retained by the contractor for a minimum of 3 years for TOP SECRET material, special access material, and CRYPTO, regardless of classification; and for SECRET material for 2 years from the date the last item recorded thereon was destroyed, downgraded to CONFIDENTIAL, declassified, dispatched outside the facility, or transferred to another accountability record.

b. Inventory/Accounting of Classified Material. When directed by a Director of Industrial Security, the contractor shall make an inventory and accounting of all TOP SECRET and SECRET material, and CRYPTO, regardless of classification, and shall submit a report of all unresolved discrepancies to the CSO. The inventory and accounting shall consist of the actual sighting of each item listed in the accountability records or an examination of the evidence of its proper disposition (the receipt, certificate of destruction, authorization to terminate from accountability, or record of downgrading or declassification); and an examination of the contents of all containers authorized for storage of classified material to ensure that all TOP SECRET and SECRET material, and CRYPTO, regardless of classification, has been entered into the accountability records.

c. Receipt and Dispatch Records. In addition to the accountability records required in paragraph a above, the contractor shall maintain a record at one or more control stations of all nonaccountable classified material received by, or dispatched from, the facility. This record shall reflect as a minimum: (i) the date of receipt or dispatch, (ii) the activity from which received or to which dispatched, (iii) the classification of the material, and (iv) a brief, unclassified description of the material. These records shall be retained by the contractor for a minimum of 2 years from the date of the last entry. However, if the contractor combines this record of receipt and dispatch with the accountability records prescribed in paragraph a above for TOP SECRET material, special access material, and CRYPTO, regardless of classification, the 3-year retention period shall apply.

d. Control Station Personnel. Employees designated by the contractor to operate a control station shall be cleared at the same level as the facility at which they are assigned. However, such personnel will be required to have a TOP SECRET clearance only if the person's duties afford him or her access to, possession of, or custody of TOP SECRET material.

e. Receipt of Classified Material. When classified material is received at the facility, either by mail, bulk shipment, or messenger, the following controls shall apply.

(1) All classified material shall be delivered unopened to personnel designated by the contractor to receive it at the control station(s). In addition, when U.S. Registered Mail, U.S. Express Mail, U.S. Certified Mail, or classified material delivered by messenger is not received directly by the

designated control station personnel, procedures shall be established to ensure that such mail is received by appropriately cleared and authorized personnel, for delivery with the inner container unopened to the control station(s). In effect, all contractor personnel who handle U.S. Registered Mail, U.S. Express Mail, or U.S. Certified Mail shall be appropriately cleared.

(2) The package shall be examined for any evidence of tampering and the classified contents shall be checked against the receipt. Evidence of tampering shall be reported immediately to the CSO, in accordance with paragraph 6a(11). Discrepancies in the contents of a package or absence of a receipt for TOP SECRET or SECRET material, and CRYPTO, regardless of classification, shall be reported immediately to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender. For purposes of positive identification, the name of the employee signing the receipt shall be printed, stamped, or typed on the receipt. In those special cases where the sender includes a receipt form with CONFIDENTIAL material, the receiver shall execute the receipt and return it to the sender, if the contents of the package are in order.

f. Production of Classified Material. When a contractor produces TOP SECRET or SECRET material, and CRYPTO, regardless of classification, accountability shall be established, as follows.

(1) TOP SECRET Documents and CRYPTO Documents, Regardless of Classification. Such documents shall be entered into the control station accountability records when the first of any of the following events occurs: (i) the document is retained after the next successive stage in its development is completed (for example notes converted to draft, final draft placed on masters, or photographic prints developed from negatives); (ii) the document, including classified working papers and drafts, is retained for more than 30 days from the date of origination; (iii) the document is reproduced for internal purposes (for example, draft review or coordination prior to preparation of final copy); or (iv) the document, regardless of its stage of development, is transmitted outside of the facility on a temporary or permanent basis.

(2) SECRET Documents. Such documents shall be entered into the control station accountability records, when the first of any of the following events occurs: (i) the document is retained as a completed document (including working papers) in excess of 30 days from the date of completion; (ii) the document is reproduced for internal purposes; (iii) the document is retained as a partially completed document on discontinuance of the work; or (iv) the document, regardless of its stage of development, is transmitted outside of the facility on a temporary or permanent basis.

(3) Other Material. TOP SECRET and SECRET material, and CRYPTO, regardless of classification, in other than documentary form, shall be entered into the control station accountability records, when the first of any of the following events occurs: (i) the material reaches the final stage in the fabrication or manufacturing process; (ii) the material is retained for more than 30 days from the date of origination; or (iii) the material, regardless of its stage of development, is transmitted outside of the facility on a temporary or permanent basis.

(4) Incorporation of Classified Material. When a classified document or other material is joined to, incorporated in, or otherwise made a part of another classified document or item of material, accountability for the incorporated document or item of material shall be terminated, and accountability for the document or item of material in which it was incorporated shall be established. The control station records shall be posted accordingly. Similarly, when a classified document is disassembled for the purpose of creating a new document or an item of material is removed from a classified assembly or end item (for example, for testing or replacement), accountability for the new material, if classified, shall be established or adjusted, as appropriate, in the control station accountability records, and the accountability for the basic document or end item shall be terminated, provided the residue is unclassified.

g. Dispatch of Classified Material. When classified material is to be dispatched from the facility, the following rules shall apply.

(1) The proposed transmittal shall be examined to ensure compliance with the preparation for transmission requirements of paragraph 17.

(2) Receipts, when required by paragraph 17a(1), shall identify the classified contents, the control station, and the name and address of both sending and receiving facilities. Receipts shall not contain classified information. A short title or abbreviation shall be substituted for a classified title.

(3) A duplicate copy of the receipt shall be retained in a suspense file until the signed copy is returned. A suspense date (normally not to exceed 30 days) shall be established, and follow-up action shall be initiated, if the signed receipt is not received within that period. If after the follow-up action a signed receipt is not returned or the addressee indicates nonreceipt of the classified material, an inquiry shall be conducted, in accordance with paragraph 7. Copies of signed receipts for classified material shall be retained at the control station for a minimum of 2 years.

h. Termination of Accountability.

(1) On notice from the CSO that accountability may be terminated for classified material determined to be lost after completion of the inquiries prescribed in paragraph 7, the contractor shall annotate the accountability records to show the date, reason, and authority for terminating accountability for the lost material.

(2) If the location or disposition of the material should subsequently be determined, the contractor shall immediately submit a report to the CSO in accordance with paragraph 6a(15), and shall reestablish accountability for, or indicate correct disposition of, the material on the control station accountability records.

13. Special Requirements for TOP SECRET.

a. It is mandatory that an up-to-date record be maintained of all persons who are afforded access to TOP SECRET information. A record shall be maintained that identifies each item of TOP SECRET material, and shows the names of all individuals given access to the item and the date (or inclusive dates) on which access by each individual occurred. In the case of employees whose duties require knowledge of the combination of containers of TOP SECRET material, the record need only identify the material, the employee(s), and the period of time during which access was available. Such records shall be retained in the appropriate control station for a period of 3 years from the date the material was destroyed, dispatched outside the facility, declassified, or downgraded. This record requirement also shall apply to those employees to whom the contractor affords visual or aural access to TOP SECRET information.

b. The number of persons afforded access to TOP SECRET information shall be kept to an absolute minimum, and each person shall be individually warned against disclosing such information to persons whose duties do not require knowledge thereof.

c. The contractor shall establish a system to preclude access to TOP SECRET material by employees working alone. Individuals with access to TOP SECRET material must be accompanied by another person cleared by the DoD who shares responsibility for ensuring against unauthorized access, improper handling, and removal of the material prior to its return to an approved storage container. In application, the policy is not intended to place undue burden on contract performance or cause excessive expenditure of funds for security equipment, personnel, or construction modifications. When adherence to this requirement would be impractical due to compelling operational requirements, the FSO may authorize exceptions on a case-by-case basis. Such relief shall be made a matter of record and shall include full justification to include the date of access and the identity of the employee permitted sole access. This requirement does not apply to situations where an employee is left alone briefly during normal working hours or to duly authorized and designated courier personnel.

d. The dissemination of TOP SECRET information should be effected orally whenever practical, without the physical transmittal of material.

e. The transmittal of TOP SECRET material shall be covered by a continuous receipt system both within and outside of the facility.

f. Each copy of a TOP SECRET document shall be numbered in series. The copy number shall be placed on accountability records and on the distribution record and receipt for each TOP SECRET document transmitted.

g. Only designated employees in the control station, cleared for access to TOP SECRET information, shall open incoming TOP SECRET transmittals. Deliveries of TOP SECRET material within the facility shall be accomplished in accordance with paragraph 17f.

h. An annual inventory and accounting of all TOP SECRET material shall be conducted in the manner prescribed by paragraph 12b.

i. TOP SECRET material shall be reproduced only with the prior written authorization of the contracting officer (see paragraph 18a).

j. Transmission of TOP SECRET material outside of the facility requires the written authorization of the contracting officer (see paragraph 17b).

k. Written approval of the contracting officer is required before disclosing TOP SECRET information to a subcontractor, vendor, or supplier (see paragraph 59a).

14. Storage.

a. Containers. Contractors shall not be eligible to receive, nor have possession of, classified material at their cleared facilities, until they have adequate and CSO approved storage capability. Classified material, when not in actual use and safeguarded as prescribed in paragraph 16, shall be stored as follows. *

(1) TOP SECRET -- Cabinets and Vaults. When not in use, TOP SECRET material shall be stored in a GSA approved security filing cabinet originally procured from a FSS supplier 6/ 7/, and bearing a GSA Test Certification Label or in a Class A vault constructed in accordance with the requirements of appendix IV 8/.

(2) TOP SECRET -- Supplemental Controls. In addition to the cabinets and vaults specified in paragraph (1) above, during nonworking hours the following area controls are required 9/.

6/ Cabinets, contractors, and prices are listed in the FSS (FSC Group 71-Part III of the GSA, Federal Supply Service). Copies of specifications and schedules may be obtained from any regional office of the GSA.

7/ Security file cabinets conforming to federal specifications bear a Test Certification Label on the locking drawer attesting to the security capabilities of the cabinet and lock. Such cabinets manufactured after February 1962 will also be marked "General Services Administration Approved Security Container" on the outside of the top drawer. Acceptable tests of the cabinets shall be performed only by a testing facility specifically approved by GSA.

8/ When authorized vaults or strongrooms are used for the storage of classified material, bin or shelf storage methods may be employed inside the vault or strongroom. In addition, any type of file cabinet or locking container may be used in the vault or strongroom to provide internal control over dissemination of the classified information.

9/ Working hours shall, for purposes of this paragraph, be considered as that period of time when: (i) there is present in the specific area in which the container is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift; and (ii) the number of employees in the scheduled work force is sufficient in number and so positioned as to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude custodians, maintenance personnel, and other individuals whose duties require movement throughout the facility.

(a) Entry to the room, building, or structure in which the container is located shall be controlled by a properly cleared, authorized employee or guard stationed so as to control admittance to the room, building, or structure, or by a lock which provides reasonable protection against surreptitious entry; and

(b) For the purpose of detecting unauthorized personnel or attempted illegal entry to the container, the interior of the room, building, or structure (whichever is controlled in accordance with paragraph (a) above) in which the container is located shall be patrolled and each container inspected at least once during each 2-hour period by a guard, one of whose principal duties is safeguarding classified information, and who is supervised by a system that provides a written record of the coverage of key points within the area; or

(c) The room, building, or structure in which the container is located, or the container itself, shall be equipped with an Intrusion Detection System (IDS), as prescribed in paragraph 35.

(3) SECRET -- Cabinets, Strongrooms, and Vaults. When not in use, SECRET material shall be stored in a cabinet or vault authorized for the storage of TOP SECRET, or in a security cabinet, strongroom, or vault as specified in paragraphs (a) through (g) below.

(a) A GSA approved cabinet originally procured from an FSS supplier and bearing a GSA Test Certification Label 6/ 7/ may be used.

(b) A Class B Vault constructed, in accordance with the requirements outlined in appendix IV 8/, may be used.

(c) A safe, steel file cabinet, or safe-type steel file container having an automatic unit locking mechanism and a built-in three-position dial-type changeable combination lock may be used. (See subparagraph (4) below.)

(d) A steel file cabinet which has five sides enclosing the drawers (including a bottom that is permanently attached by welding, rivets or peened bolts so it may not be removed without leaving visible evidence of entry) secured by a rigid metal bar 10/ and a three-position dial-type changeable combination padlock listed on the GSA Qualified Products List as meeting the requirements of Federal Specification FF-P-110 may be used. (See subparagraph (4) below). *

10/ The keepers of the rigid metal bar shall be secured to the cabinet by welding, rivets, or bolts, so that it cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely, so that their contents cannot be removed without forcing open the drawer. *

1 Three position dial-type changeable combination padlocks which do not meet the requirements of FF-P-110, in use at the present time, may remain in use until replacement is necessary, or until July 1, 1991, whichever occurs first. 11/

2 These cabinets will not be authorized for storage of SECRET information effective July 1, 1998, 11/ unless the cabinets themselves are alarmed, or they are placed in an alarmed area, closed area, or strongroom, or are under constant visual surveillance by appropriately cleared personnel during non-working hours. The phase-in period only pertains to facilities cleared prior to June 20, 1988. All facilities cleared after that date must conform to these standards prior to receiving approval to safeguard SECRET material.

(e) A Class C Vault constructed in accordance with the requirements of appendix IV 8/. (See subparagraph (4) below.)

(f) A strongroom may be used, provided the strongroom is supplementally controlled by a regularly scheduled 2-hour guard patrol, or is equipped with an a IDS as prescribed in paragraph 35. (See paragraph F, appendix IV, for construction requirements.)

(g) A steel container in a desk pedestal, which encloses the container on five sides and is riveted or bolted to the desk may be used, provided the exposed face of the container is secured by a steel bar and a three-position dial-type changeable combination padlock 10/. (See subparagraph (4) below.)

(4) SECRET -- Supplemental Controls. In addition to the cabinets and vaults specified in paragraphs (3)(c), (d), (e), and (g) above, during nonworking hours the following area controls are required 9/.

(a) Entry to the room, building, or structure in which the container is located shall be controlled by a properly cleared, authorized employee or guard stationed so as to control admittance to the room, building, or structure, or by a lock that provides reasonable protection against surreptitious entry; or by a properly cleared guard stationed at each unsecured perimeter entrance to a complex 12/ that is enclosed by a physical barrier, and provided further that the area is patrolled adequately to provide reasonable opportunity to detect unauthorized personnel; and

(b) For the purpose of detecting unauthorized personnel or attempted illegal entry into the room, building, or structure (whichever is controlled in accordance with paragraph (a) above) in which the container is located, the area shall be patrolled at least once during each 4-hour period by a properly cleared, authorized employee or guard. One of this

---

11/ Case-by-case exceptions may be granted by the CSO.

12/ A complex is a facility or any element thereof which consists of one or more buildings or structures physically enclosed within a common perimeter barrier supplemented by protective measures, which prevent unauthorized access and control authorized access.

best copy available

employee's or guard's duties must be safeguarding classified information and he or she must be supervised by a system that provides a written record of the coverage of key points within the area; or

(c) The room, building, or structure in which the container is located, or the container itself, shall be equipped with an IDS, as prescribed in paragraph 35.

(5) CONFIDENTIAL -- Cabinets, Strongroom, and Vaults. When not in use, CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material; however, supplemental controls are not required.

b. Bulky Material. When it is impractical to store classified material because of its nature, size or unique characteristics, in accordance with paragraph a above, the contractor shall safeguard such material by control of the area in which it is located, to the extent required by section IV. If it is impractical to safeguard the material in accordance with section IV, the contractor shall develop appropriate alternative control procedures and provide them to the CSO for approval.

c. Supervision of Storage Containers. Only a minimum number of authorized persons shall possess the combinations to the storage containers or have access to the information stored therein. To facilitate investigation of a container found open and unattended, a record shall be maintained of the names and addresses of persons having knowledge of the combination. Cabinets, vaults, and other containers in which classified material is stored shall be kept locked, when not under the direct supervision of an authorized person entrusted with the combination or the contents. In the case of a one-person facility, the management official shall inform the CSO of the combination of the container. The combination shall be classified, in accordance with paragraph 51, shall be placed in a sealed envelope marked, "to be opened upon death or incapacitation of (name of management official)," and shall be transmitted to the CSO, in accordance with paragraph 17. In addition, conspicuously displayed on the outside of the container shall be a notice to contact the CSO, prior to opening or moving the container. This notice shall contain the mailing address of and an appropriate telephone number at the CSO. The above provisions pertaining to one-person facilities do not apply to cleared one-person facilities of an MFO. For such facilities, provisions should be made in the HOF SPP for affixing an appropriate notice on the outside of the cabinet, and for furnishing the combination to the FSO of the HOF who shall be identified as the official to contact rather than the CSO.

d. Protection During Nonworking Hours. Unless specified in a UA contract, a contractor shall not be required to establish additional controls over classified material stored in accordance with paragraph a above.

e. Removal to Residence. Although the contractor may have provided for adequate storage facilities at the respective residences of his officers, directors, and other employees, removal of classified materials to such dwellings for "after hours" work as a convenience to such persons is not authorized.

These facilities, provided they meet the requirements of this manual, may be utilized for temporary storage purposes only in connection with authorized travel when the individual, in order to accomplish the objectives of the trip, is authorized to carry classified material as prescribed in paragraph 17h, or in other cases of necessity on approval by an official of the facility who was cleared in connection with the granting of the FCL. In no case will TOP SECRET material be removed to a private residence without: (i) the written authorization of the contracting officer in accordance with paragraph 17b, and (ii) approval of the CSO as to the security controls to be maintained over the TOP SECRET material while it remains outside of the facility.

f. Repair of Damaged Security File Cabinets. Neutralization of lockouts or repair of any damage which affects the integrity of a security file cabinet approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance, neutralization of lockouts, and repair of perforations.

(1) A GSA approved security file cabinet is considered to have been restored to its original state of security integrity if:

(a) all damaged or altered parts (for example locking drawer and drawer head) are replaced with manufacturer's replacement or identical cannibalized parts, or

(b) when a container has been drilled immediately adjacent to or through the dial ring to neutralize a lockout, the replacement lock is equal to the original equipment and the drilled hole is repaired with a tapered case-hardened steel rod (for example, dowel and drill bit) with a diameter slightly larger than the hole, and of such a length that when driven into the hole there shall remain at each end of the rod a shallow recess of not less than 1/8 inch deep, nor more than 3/16 inch, to permit the acceptance of substantial welds, and be welded both on the inside and outside surfaces. The outside of the drawer head shall then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged part (for example, new lock.)

(2) If damage to a GSA approved or other approved security file cabinet is repaired with welds, rivets, or bolts, which cannot be removed and replaced without leaving evidence of entry, the cabinet thereafter may be used for storage of CONFIDENTIAL material or SECRET material with supplemental controls as outlined in paragraph 14(a)4. If the damage is repaired using methods other than those specified in paragraph (1) above or this paragraph, use of the cabinet shall be limited to unclassified material.

g. Damage to Approved File Cabinets 7/. A list shall be maintained by the FSO of all approved file cabinets which have sustained damage other than normal marring or scratching from use. Each cabinet listed shall be identified by giving its location and a description of the damage. There shall also be on file a signed and dated certification, provided by the repairer, setting forth the method of repair used. The list and certification shall be retained for the life of the file cabinet and shall be available for review during recurring security inspections. Each such cabinet shall have a label posted on the inside of the top drawer to indicate the highest category of classified material which may be stored therein. If the damage affects the integrity of a GSA approved cabinet, the GSA Approved Security Container Label and the GSA Test Certification Label shall be removed. However, these labels may be retained by the FSO for a period of 30 days for those GSA approved cabinets designated for repair to restore their original integrity. If integrity is not restored within 30 days, the labels shall be destroyed. When a GSA approved cabinet is repaired in accordance with --

(1) Paragraph f(1)(a) above, the replacement locking drawer will have its GSA Test Certification Label affixed. In this case the retained GSA Approved Security Container Label shall be affixed to the outside of the top drawer and the retained GSA Test Certification Label shall be destroyed.

(2) Paragraph f(1)(b) above, the retained GSA Approved Security Container Label shall be affixed to the outside of the top drawer, and the GSA Test Certification Label shall be affixed to the inside of the locking drawer.

15. Alternate Storage Locations.

a. General. Material classified no higher than SECRET, requiring protection in the interest of national defense and essential to continuity of production operations, may be duplicated and stored in an alternate location, provided the contracting officer approves the use of such storage for information pertaining to the contract. The provisions of section VI shall apply to the procurement of this service. Acceptable alternate storage locations are cleared facilities of: (i) a parent, a subsidiary, or another facility of an MFO; (ii) a bank offering safe deposit box/vault facilities; or (iii) a company providing a protective storage service.

b. Security Clearance Requirements. The alternate storage location shall be a cleared facility. PCL requirements will depend on the type of service provided. Where the alternate storage facility is required to provide both secure storage and other services requiring access to the classified information, PCL's are required for employees whose duties will involve access to the classified material or responsibility for providing security protection for the classified material. When the facility is to provide only secure storage space, PCL's are required only for those personnel whose duties involve responsibility for security protection of the classified material.

c. Records. When the alternate storage facility provides both secure storage and file service for the classified information, all of the security requirements prescribed in this manual shall apply. When the alternate storage facility provides only secure storage service, accountability for the alternate files shall be maintained on a separate record by the facility which deposits the material.

d. Containers. When the services of a bank are utilized, safe deposit boxes will be considered equivalent to FSS security cabinets, provided the prime contractor:

(1) controls the keys to the safe deposit box in the same manner that combinations to storage containers are safeguarded, in accordance with paragraph 51;

(2) utilizes only cleared employees, whose signatures are on file with the bank, to deposit and remove classified material; and

(3) ensures that established procedures preclude access to the classified information by employees of the bank.

16. Safeguards During Use. Classified materials, when not safeguarded as provided for in paragraphs 14a or b, or 34, and when in actual use by authorized personnel, shall be protected as follows:

a. kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security controls over the material;

b. covered, turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present; and

c. returned to storage containers as soon as practical after use.

17. Transmission.

a. Preparation for Transmission of TOP SECRET, SECRET, and CONFIDENTIAL Material.

(1) Outside of a Facility. TOP SECRET, SECRET, and CONFIDENTIAL material to be transmitted outside of a facility shall be enclosed in opaque inner and outer containers, except as provided for in paragraph (b), (c), or (d) below. If the classified material is printed or written, and is of such size as to permit the use of envelopes for wrapping, the classified information shall be protected from direct contact with the inner container by a cover sheet or by folding inward. Except as indicated in paragraph (e) below, the inner container shall be addressed, return addressed, carefully sealed, and shall be plainly and conspicuously marked with the classification of the contents and, if appropriate, with the notations required by paragraphs 11b(8), 68a, and 123. The outer container shall be addressed, return addressed, and carefully sealed with no markings or notations to indicate that the contents are classified. If the outer container is not sufficiently opaque to prevent the classification markings on the inner cover from being visible, the inner container shall be wrapped with sufficient paper to conceal the markings. If the classified material is of a size, bulk, weight, or nature which precludes wrapping as described above, materials used for the packaging shall be of such strength and durability as to provide protection while in transit. To prevent items from breaking out and to facilitate the detection of tampering with the container, the following will be used, whenever practical: seals, kraft paper, kraft tape laminated with asphalt and containing rayon fibers (snake type) or nylon sensitive tape, puncture resistant material, wire mesh, or other knife-slash resistant material. As long as the material is enclosed in a double container, the material may be wrapped or boxed in paper, wood, metal, or a combination thereof. When transmitting TOP SECRET and SECRET material the inner container shall contain a receipt form which identifies the addressor, the addressee, and the contents by unclassified or short title. Where this is not practical, the receipt shall be sent to the proposed recipient with the advance notice of shipment required by paragraphs c(5)(c) and d(3)(d) below, or hand-carried by a responsible employee

designated to accompany the classified shipment to its destination. When transmitting CONFIDENTIAL material, a receipt form is not required. Special provisions for the packaging of classified material are as follows.

(a) The transmission of written materials of different classifications, for example, the inclusion of CONFIDENTIAL and UNCLASSIFIED with SECRET in a single package, should be avoided. However, when written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container, and the receipt required by paragraph (1) above, shall be enclosed. The inner envelope or container shall be marked with the highest classification of its contents.

(b) If the classified material is an internal component of a packageable item of equipment with an outside shell or body, which is not classified and which completely shields the classified aspects of the item from view, the shell or body may be considered as the inner container.

(c) If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable, such as a missile, the outside shell or body of the item may be considered as the outer container, provided the shell or body is not classified.

(d) If the classified material is an item of equipment that is not reasonably packageable and the shell or body is classified, it shall be draped with an opaque covering that will conceal all classified features. Such coverings must be capable of being secured so as to prevent inadvertent exposure of the item.

(e) Specialized shipping containers, including closed cargo transporters, may be used in lieu of the above packaging requirements. In such cases the container may be considered to constitute the outer container.

(f) The address may be omitted from the inner and outer container for shipment in full truckload lots, when such an exception is contained in the provisions of the contract. The DFARS requires that complete consignment and marking instructions, to the extent known at the time the contract is awarded, be included in the contract to assist in ensuring delivery of items to proper destinations without delay. It further requires that additional consignment instructions be furnished to the contractor as soon as they become known. Under no circumstances will the outer container, or the shipping document attached to the outer container, reflect the classification of the contents or the fact that the contents are classified.

(2) Additional Requirements for SECRET Material to be Shipped by Commercial Carrier 13/. SECRET material to be transmitted outside a facility by commercial carrier shall be prepared for transmission to afford additional protection against pilferage, theft, and compromise. Specific provisions for shipment of SECRET material are as follows.

13/ Commercial carriers have been issued instructions in the "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information," DoD 5220.22-C, applicable to their responsibilities for transmissions of SECRET controlled shipments.

(a) Except as authorized in paragraph 17a(1), SECRET material shall be shipped in hardened containers (see paragraph 3as), unless specifically authorized otherwise by the contracting officer or his or her designated representative.

(b) Carrier equipment shall be sealed by the shipper, or at his or her direction, when there is a full carload, a full truckload, exclusive use of the vehicle, or a closed and locked compartment of the carrier's equipment is used. The seals shall be numbered and the number indicated on all copies of the BL. When seals are used, the BL shall be annotated substantially as follows:

> DO NOT BREAK SEALS EXCEPT IN CASE OF EMERGENCY OR UPON PRIOR AUTHORITY OF THE CONSIGNOR OR CONSIGNEE. IF FOUND BROKEN OR IF BROKEN FOR EMERGENCY REASONS, APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY BOTH THE CONSIGNOR AND THE CONSIGNEE. 14/

(3) Within a Facility. TOP SECRET, SECRET, and CONFIDENTIAL material shall be prepared for transmission within a facility in such a manner as to ensure a degree of security protection adequate for the method of transmission to be used, using guidance contained in paragraph (1) above. Material does not require double wrapping for intraplant transmission. However, in all cases, adequate measures shall be taken to protect against unauthorized disclosure of classified information.

b. Method of Transmission of TOP SECRET Material Outside a Facility. 15/ When a contractor is authorized in writing, by the contracting officer or his or her designated representative, TOP SECRET material may be transmitted by: * * *

(1) Specifically designated escort or courier cleared for access to TOP SECRET information (military, U.S. civilian employee, or a responsible employee designated by the contractor, except that the contractor employee shall not carry classified material across international boundaries).

(2) By electrical means in a CRYPTOSYSTEM approved for encryption of TOP SECRET information.

(3) Defense Courier Service (DCS) in accordance in accordance with the instructions of the contracting officer; (For all DoD or other U.S. Government agencies which issue contracts providing for DCS service, the * * *

14/ In such cases the SECRET shipment shall be routed via a cleared commercial carrier under a tariff, tender, or contract that provides PSS in accordance with the DoD 5220.22-C.

15/ Special transmission requirements and procedures for the Secure Telephone Unit, STU III, are outlined in Appendix XVIII.

Contracting Office's Authorizing Representative (COAR) must submit a letter to Headquarters, DCS, requesting approval for service. The letter should include the following: (i) name and complete address of the contractor; (ii) contract number; (iii) expiration date of the contract; (iv) type of account required (SCI/non-SCI/COMSEC); (v) expected frequency of service; (vi) anticipated volume of material; (vii) whether material is to be shipped to/from contractor facility; and (viii) name, address and telephone of COAR. The letter of request shall be sent to:

Commander
Defense Courier Service
ATTN: DOC
Ft. George G. Meade, Maryland 20755-5370.)

(4) Under no circumstances shall TOP SECRET material be transmitted through the U.S. or company mail channels.

c. Method of Transmission of SECRET Material Outside a Facility. 15/ SECRET material may be transmitted by one of the following means within and between the U.S., Puerto Rico, or a U.S. possession or trust territory.

(1) SECRET material may be transmitted by one of the means established for TOP SECRET.

(2) SECRET material may be transmitted by U.S. Registered Mail, including U.S. Registered Airmail, through U.S. civil postal facilities or Army, Navy, or Air Force postal facilities. Addresses may be obtained from the "DoD Activity Address Directory," DoD 4000.25-D (a reference copy is located at the CSO), or from the ACO/PCO. A copy of DoD 4000.25-D may also be purchased from the GPO.

(3) SECRET material may be transmitted by appropriately cleared employees of the contractor who have been designated as couriers or escorts and briefed in their responsibilities by a responsible official delegated authority in such matters in the facility SPP. When couriers or escorts are used, the SECRET material must remain in their personal custody and control at all times (see paragraph 17h). The commercial conveyance used by the courier or escort is not required to have an FCL. (See Appendix IX for use of escorts for classified shipments and Appendix X for hand-carrying of classified material aboard commercial passenger aircraft).

(4) SECRET material, including computer data, may be transmitted by electrical means over approved CRYPTOGRAPHIC communication circuits (telephone, wire, radio, or an intercommunication system) provided such transmission is in consonance with the telecommunications security provisions of the contract or as otherwise authorized by the contracting activity. NOTE: National Communications Security Instruction (NACSI) 6002 requires U.S. Government agencies to identify classified or otherwise sensitive Government information related to their contracts and to require their contractors to secure such information when it is telecommunicated. DoD Instruction 5210.74, "Security of Defense Contractor Telecommunications" implements this policy in the DoD.

(5) SECRET material may be transmitted by commercial carriers 16/ * (air or surface) only when the size, bulk, weight, nature of the shipment, shipping costs, or escort considerations make the use of the foregoing methods impractical. Only qualified carriers (see paragraph 3bs) will be used for the transmission of SECRET material. When the services of a commercial carrier are required, the contractor as consignor shall be responsible for the following.

(a) The contractor shall utilize a qualified carrier selected by the U.S. Government that will provide a single line service from point of origin to destination, when such service is available, or by such transshipping procedures as may be specified by the U.S. Government; and

(b) The contractor shall request routing instructions, including designation of a qualified carrier, from the contracting officer or designated representative (normally the government transportation officer). The request shall specify that the routing instructions are required for the shipment of SECRET material via Protective Security Service (DO NOT ABBREVIATE THIS) and include the point of origin and point of destination; or

(c) As an exception to the general requirements enunciated above, if time is of the essence and the total shipment weighs less than 200 pounds gross, the contractor, as consignor, may make arrangements directly with a cleared commercial carrier to provide PSS for the transporting of the SECRET shipment when a CBL is to be used. This exception may not be utilized for COMSEC or SENSITIVE COMPARTMENTED INFORMATION (SCI) material without the approval of the PCO. Under this exception the contractor must specify to the commercial carrier that SECRET material is to be shipped and that PSS is required. The points of origin and destination must also be provided. Verifications of the clearance of the commercial carrier and the fact that it provides PSS are to be obtained from the CSO of the HOF of the carrier prior to release of any classified material; and

(d) The contractor shall notify the consignee (including a U.S. Government transshipping activity) of the nature of the shipment, the means of the shipment, numbers of the seals, if used, and the anticipated time and date of arrival by separate communication at least 24 hours in advance (or immediately on dispatch if transit time is less than 24 hours) of the arrival of the shipment, in order that the consignee may take appropriate steps to receive and protect the shipment. This notification shall be addressed to the appropriate organizational entity in the same manner as provided in paragraph 17k and not to an individual. Request the consignee activity (including a military transshipping activity) to notify the consignor of any shipment not received within 48 hours after the estimated time of arrival indicated by the consignor. In addition, the consignor shall annotate the BL: "CARRIER TO NOTIFY THE CONSIGNOR AND CONSIGNEE (Telephone Numbers) IMMEDIATELY IF SHIPMENT IS DELAYED BECAUSE OF AN ACCIDENT OR INCIDENT. IF

16/ Commercial carriers may be used only within and between the 48 contiguous States and the District of Columbia or wholly within Alaska, Hawaii, Puerto Rico, or a U.S. possession or trust territory.

NEITHER CAN BE REACHED, CONTACT (Enter appropriate HOTLINE Number from Appendix XV). USE HOTLINE NUMBER TO OBTAIN SAFE HAVEN OR REFUGE INSTRUCTIONS IN THE EVENT OF A CIVIL DISORDER, NATURAL DISASTER, CARRIER STRIKE OR OTHER EMERGENCY." On receipt of a report from either the consignor or the carrier, the consignor shall immediately request the carrier to trace the shipment and shall notify his or her CSO of the delay in the delivery of the classified material and the circumstances as known to the consignor. Subsequent developments concerning the delayed shipment shall also be reported to the CSO. A copy of the report shall be submitted to the contracting officer concerned or his or her designated representative. The consignee, consignor, and carrier are required to take similar inquiry and reporting action if a shipment is received with broken seals, or the numbers on the seals do not match those on the advance notice of shipment.

(6) SECRET material may be transmitted by a commercial messenger service which has been granted a SECRET FCL and is engaged in the intra-city/local area delivery (same day delivery only) of classified material between cleared contractors, or between cleared contractors and a UA and/or the U.S. Post Office. Transmission of COMSEC information and SCI will not be released to a commercial messenger service without contracting officer approval. *

(7) SECRET material may be transmitted by such other methods directed through specific instructions from the contracting officer or his or her designated representative, because of special considerations or the nature of the shipment (for example, explosives, high priority items, nuclear weapons or direct shipments between military installations) 17/. *

d. Method of Transmission of CONFIDENTIAL Material Outside a Facility 17/. Such material may be transmitted by one of the following means within and between the U.S., Puerto Rico, or a U.S. possession or trust territory. *

(1) One of the means established for SECRET in paragraphs c(1), (2), (3), (4), (6), and (7) above 16/ may be used.

(2) U.S. Express Mail 18/ or U.S. Certified Mail for CONFIDENTIAL material may be used. However, U.S. Registered Mail shall be used for

---

17/ When a shipment by truck is contemplated for classified CM (CONFIDENTIAL or SECRET), the contracting officer will issue specific shipping instructions requiring a driver holding a final SECRET clearance in addition to the military escort normally provided for such shipments.

18/ U.S. Express Mail is a premium mail service consisting of both programmed and regular service. The service is intended for, but not limited to use by, the business mailer or other large volume users of the mails. The service is a high-speed intercity delivery system that usually can negate the requirement to hand-carry CONFIDENTIAL material in cases of short notice. Additional information is available through a local postal customer service representative regarding the specific options that are available.

transmittal of such material between any of the following points: the CONUS, Alaska, Hawaii, Puerto Rico, or a U.S. possession or trust territory. Addresses may be obtained from the "Department of Defense Activity Address Directory," DoD 4000.25-D (a reference copy is located at the CSO), or from the ACO/PCO. A copy of the DoD 4000.25-D may be purchased from the GPO.

(3) A commercial carrier 16/ (air or surface) may be used only when the size, bulk, weight, nature of the shipment, shipping costs, or escort considerations make the use of the foregoing methods impractical. The commercial carrier must be authorized by law, regulatory body, or regulation to provide the required transportation service and a determination must be made by MTMC that the carrier has a tariff, government tender, agreement, or contract that provides a CSS. An FCL is not a requirement. The foregoing information may be obtained from the contracting officers or their designated representatives. In addition to the aforementioned coordination with the contracting officers or their designated representatives, the contractor, as consignor shall:

(a) utilize containers of such strength and durability as to provide security protection to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container while in transit;

(b) indicate on the BL, "Constant Surveillance Service Required" -- in addition, the consignor shall annotate the BL: "CARRIER TO NOTIFY THE CONSIGNOR AND CONSIGNEE (Telephone Numbers) IMMEDIATELY IF SHIPMENT IS DELAYED BECAUSE OF AN ACCIDENT OR INCIDENT. IF NEITHER CAN BE REACHED CONTACT (Enter appropriate HOTLINE number from Appendix XV). USE HOTLINE NUMBER TO OBTAIN SAFE HAVEN OR REFUGE INSTRUCTIONS IN THE EVENT OF A CIVIL DISORDER, NATURAL DISASTER, CARRIER STRIKE OR OTHER EMERGENCY;"

(c) instruct the carrier to ship packages weighing less than 200 pounds gross in a closed vehicle or a closed portion of the carrier's equipment; and

(d) notify the consignee (including a U.S. Government transshipping activity) of the nature of the shipment, the means of shipment, and the anticipated date and time of arrival by separate communication at least 24 hours in advance (or immediately on dispatch if transit time is less than 24 hours) of the arrival of the shipment in order that the consignee may take appropriate steps to receive and protect the shipment. This notification shall be addressed to the appropriate entity in the same manner as provided in paragraph 17k and not to an individual. Request the consignee (including a military transshipping activity) to notify the consignor of any shipment not received within 48 hours after the estimated time of arrival indicated by the consignor. On receipt of such notice, the consignor shall immediately request the carrier to trace the shipment and shall notify his or her CSO, in accordance with paragraph 6a(10), of the delay in the delivery of the classified material and the circumstances as known to the consignor. Subsequent developments concerning the delayed shipment shall also be reported to the CSO. A copy of the report shall also be submitted to the contracting officer concerned or his or her designated representative, for forwarding to the MTMC.

e. Method of Transmission of SECRET and CONFIDENTIAL Material Outside of Areas Enumerated in Paragraphs 17c and d. SECRET and CONFIDENTIAL material shall be transmitted only under the provisions of the contract or with the written authorization of the contracting officer. However, when the classified material had previously been authorized for export under a State Department license or letter, the contractor shall notify the contracting officer of the classified material to be transmitted outside of the areas enumerated in paragraphs c and d above. A contractor shall not transmit classified material directly to a foreign government or firm. The only exception to this would be when a foreign government, with whom the U.S. has entered into a reciprocal agreement pertaining to the filing of classified patent applications in the respective countries, has authorized its U.S. patent agent to return its foreign classified information directly to that foreign government. Except as noted above, transmission shall take place between the contractor and a designated U.S. Government representative for forwarding to the foreign activity. This is known as transmission by government-to-government channels. Transmittal arrangements shall be made by the CSO, when the foreign firm or government has awarded a contract to the U.S. contractor. When authorized, SECRET and CONFIDENTIAL material shall be transmitted by one of the following means.

(1) SECRET and CONFIDENTIAL material shall be accompanied by a contractor employee, courier or escort, who is cleared for access to the classified information involved and who has been designated by the contractor, provided: (i) the classified material is not transported across international borders (this does not preclude use of regularly scheduled nonstop flights on U.S. carriers between the U.S. mainland and Alaska, Hawaii, Puerto Rico, or U.S. possessions or trust territories); (ii) time limitations do not permit the use of U.S. Government channels; (iii) an appropriate courier or escort authorization is issued to the employee; (iv) the transmission is begun and completed during normal daytime duty hours of the same day and is by surface means only and within the national borders of the country within which the transmission takes place; and (v) the employee can comply with the specific security instructions for the safeguarding of classified material involved; that is, storage at a U.S. Government installation within the country concerned.

(2) SECRET and CONFIDENTIAL material shall be accompanied by a U.S. Government civil service employee or military person who is cleared for access to the level of the classified information involved and who has been designated by the contracting officer. (Appropriately cleared officers of the Department of Navy, Military Sea Transportation Service Civilian Marine Personnel, may also be designated as escorts by the contracting officer.) Foreign carriers may not be utilized, unless the designated escort has continuous physical control of the material being transported.

(3) SECRET and CONFIDENTIAL material shall be transmitted by registered mail through U.S. Army, Navy, or Air Force postal facilities. If the intended recipient is not authorized to receive classified material through APO channels, arrangements shall be made with an activity which is so authorized to receive and hold the classified material pending pickup by the intended recipient.

(4) SECRET and CONFIDENTIAL material shall be transmitted by U.S. and Canadian registered mail with registered mail receipt to and from Canada in accordance with instructions from the contracting officer and via a U.S. or a Canadian government activity.

(5) Certain SECRET and CONFIDENTIAL material may be transmitted by DCS in accordance with specific instructions from the contracting officer.

(6) SECRET and CONFIDENTIAL material shall be transmitted in accordance with specific instructions from the contracting officer, whenever the nature of the classified shipment does not lend itself to transmission by any of the above methods. In such cases, the procedures for advance notice to consignee, reporting of delayed receipt, and so on set forth in paragraph c(5)(d) above apply.

f. Method of Transmission of TOP SECRET, SECRET, and CONFIDENTIAL Material Within a Facility. This material may be transmitted within a facility by a responsible employee designated by the contractor who has been cleared for access to the category of classified information involved. Also, a responsible subcontractor guard who is employed on a full-time basis at the facility, possesses an appropriate PCL, and has been designated and briefed by the contractor, may be utilized to transmit SECRET and CONFIDENTIAL material. The classified material shall remain under the direct surveillance of the designated individual at all times. This material may be transmitted by electrical means over approved CRYPTOGRAPHIC communications circuits provided such transmission is in consonance with the telecommunications security provisions of the contract or as otherwise authorized by the contracting activity.

g. Reserved.

h. Protection En Route by Contractor Employees. When employees designated by the contractor are used to transmit or carry classified material, the storage provisions of paragraph 14 shall apply at all stops en route to destination, unless the material is retained in the personal possession of the employee at all times. This involves constant surveillance by the employee who is in a physical position to exercise direct security controls over the material. The hand-carrying of classified material on trips that involve an overnight stopover is not permissible, unless arrangements are made in advance of departure for overnight storage of the hand-carried classified material at a U.S. Government installation or a cleared contractor facility. The hand-carrying of classified material shall not be authorized when there is doubt as to whether the material can be properly handled and protected. Additional special requirements for hand-carrying classified material aboard commercial passenger aircraft are contained in appendix X.

i. Additional Protection in Connection With Visits. When classified material, other than TOP SECRET, is required on a visit, such material shall be addressed by the contractor to his or her employee making the visit and shall be transmitted in accordance with paragraphs c(2) or d(2) above to the destination being visited to be held for the employee. This method shall also be used for the return of the material. However, if contractors determine that time limitations do not permit mailing materials required during visits, they may authorize the employees concerned to carry the classified material, subject to the provisions of paragraph h above. An inventory of the material shall be made prior to departure and retained at the control station. A copy of the inventory shall be carried by the employee. Only that classified material absolutely essential to the purpose of the visit may be carried by the employee. On the employee's return from the visit, an inventory shall be made of the material for which he or she is charged. If, in connection with the purpose of the visit, classified material is not returned to the facility, a receipt shall be obtained and the transaction shall be recorded in the records of the control station, in accordance with paragraph 12. However, should there be a need to leave CONFIDENTIAL material at the facility visited, a receipt is not necessary, except if otherwise required in accordance with paragraph 12.

j. COMSEC Information. Classified COMSEC information shall be transmitted as prescribed in the "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information" (CSISM), DoD 5220.22-S.

k. Addressing Mail or Shipments of Classified Material. Except as provided below, mail or shipments containing classified material shall be addressed to the Commander or Head of the UA activity or installation (Commander, Commanding Officer, Director, TO, or similar designation) or to the cleared facility concerned, using the appropriate business name and address, and not to an individual. This does not prevent use of office code letters or numbers, or such phrases in addition to the address as, "ATTN: Research Dept.," or similar aids in expediting internal routing.

(1) When it is considered desirable or appropriate to direct SECRET or CONFIDENTAL material to the attention of a particular employee of a facility or UA, other than to a consultant as prescribed below, the identity of the intended recipient shall be indicated on an attention line on the inner container or on an attention line placed in the letter of transmittal. If such mail is to be delivered directly to the specified employee, a procedure shall be established to ensure that all classified enclosures are promptly entered into the facility's document control system in accordance with paragraph 12.

(2) When transmitting SECRET or CONFIDENTIAL material to an individual operating as a cleared facility or engaged as a Type B or C Consultant, or to any facility at which only one employee is assigned, the contractor shall specify on the outer container: "TO BE OPENED BY ADDRESSEE ONLY." Further, the outer container shall be annotated: "Postmaster -- Do Not Forward. If undeliverable to Addressee, Return to Sender." Postal regulations allow "Restricted Delivery" mail to be delivered to the addressee or to an agent the addressee has authorized in writing to receive "Restricted Delivery" mail. In all such instances, only appropriately cleared personnel shall be designated as agents for the addressee. Type C Consultants shall make arrangements to ensure that all incoming U.S. Certified Mail, U.S. Registered Mail, and U.S. Express Mail addressed to them in their capacity as independent consultants is delivered unopened to them personally through their employer's mail distribution system before entering it into their employer's document control system.

l. RESTRICTED DATA and FORMERLY RESTRICTED DATA. RESTRICTED DATA and FORMERLY RESTRICTED DATA shall not be transmitted or otherwise made available to any regional defense organization or foreign government, except under the provisions of the Atomic Energy Act of 1954, as amended, and in accordance with instructions issued by the contracting officer concerned.

m. Transmission of Classified Material to Foreign Governments: After a determination by designated U.S. Government officials that classified information or material may be released to a foreign government, the material shall be transferred between authorized representatives of each government. Each contract, agreement, or other arrangement that involves the release of classified material to foreign entities as freight to be moved via truck, rail, aircraft, or ship shall either contain transmission instructions or a separate transportation plan approved by the appropriate DoD security and transportation officials prior to release of the material. The approving official will provide a copy of the approved transportation plan or the transmission instructions to the appropriate DIS CSO for inspection purposes.

(1) Classified material released to a foreign government shall be delivered or transmitted only to a properly cleared individual who has been designated in writing by the recipient government as its officer, agent, or employee (hereafter referred to as the designated representative). Foreign governments may designate a cleared freight forwarder as their agent. The designated representative must assume full security responsibility for the material on behalf of the foreign government. The foreign government's designated representative is required to execute a receipt for all the material, regardless of classification. The signature tally used with CSS or PSS service may serve as the receipt when freight forwarders are employed.

(2) Classified material that cannot be transferred directly to a foreign government's designated representative pursuant to subparagraph (1) above shall be transmitted to the foreign government at one of the following locations:

(a) an embassy, consulate, or other official agency of the recipient government having extraterritorial status in the U.S., or

(b) a U.S. Embassy or a U.S. military organization in the recipient country or in a third-party country, if applicable, for subsequent delivery to a designated representative of the intended recipient government.

(3) The shipment of classified material as freight via truck, rail, aircraft, or ship shall be in compliance with the following:

(a) Shipments Resulting from Foreign Military Sales (FMS): DoD officials authorized to approve an FMS transaction that involves the delivery of U.S. classified material to a foreign purchaser shall, at the outset of negotiation or consideration of proposal, consult with DoD transportation authorities (Military Traffic Management Command, Military Sealift Command, Military Airlift Command, etc.) to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the U.S. will use the DTS to deliver classified material to the recipient government. If, in the course of FMS case processing, the foreign purchaser proposes to take delivery and custody of the classified material in the U.S. and use its own facilities and transportation for onward shipment to its territory, the foreign purchaser or its designated representative shall be required to submit a transportation plan or transmission instructions for DoD review and approval. The plan or separate instructions shall specify the storage facilities, delivery and transfer points, carriers, couriers or escorts, and methods of handling to be used from the CONUS point of origin to the final destination and return shipment when applicable (See appendix XVII). Security officials of the DoD component that initiates the FMS transaction shall evaluate the transportation plan or transmission instructions to determine whether they ensure protection of the classified material involved. Unless the DoD component initiating the FMS transaction approves the transportation plan or instructions as submitted, or they are modified to meet U.S. security standards, shipment by other than DTS shall not be permitted. Transmission instructions or the requirement for an approved transportation plan shall be incorporated into the security requirements of the "United States Department of Defense Offer and Acceptance" (DD Form 1513).

(b) Shipments Resulting from Commercial Sales: Classified shipments resulting from commercial sales must comply with the same security standards that apply to FMS shipments. To obtain approval of the transportation plan or transmission instructions defense contractors must consult with the purchasing government and the appropriate DIS CSO prior to consummation of a commercial contract that will result in the shipment of classified material.

(c) Delivery Within the U.S., Its Territories, or Possessions: Delivery of classified material to a foreign government at a point within the United States, its territories, or its possessions, shall be made only to a person or activity identified in writing by the recipient government as its designated representative as specified in subparagraph (1) above. The only authorized delivery points are:

1 An embassy, consulate, or other official agency under the control of the recipient government.

2 Point of origin. When a designated representative of the recipient government accepts delivery of U.S. classified material at the point of origin (for example, a manufacturing facility or depot), the DoD official who transfers custody shall obtain a receipt for the classified material and assure that the recipient is cognizant of secure means of onward movement of the classified material to its final destination, consistent with the approved transportation plan or transmission instructions.

3 Military or commercial ports of embarkation (POE) that are recognized points of departure from the U.S., its territories, or possessions, for onloading aboard a ship, aircraft, or other carrier authorized under subparagraph 17n below. In these cases, the transportation plan or transmission instructions shall provide for U.S.-controlled secure shipment to the CONUS transhipment point and the identification of

a secure storage facility, government or commercial, at or in proximity to the POE. A DoD official authorized to transfer custody is to supervise or observe the onloading of FMS material being transported via the DTS and other onloading wherein physical and security custody of the material has yet to be transferred formally to the foreign recipient. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility provided by the U.S. shipper (government or contractor); or segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE; or held in the secure storage facility (government or commercial) designated in the transportation plan/instructions.

4 A freight forwarder facility that is identified by the recipient government as its designated representative and that is cleared to the level of the classified material to be received. In these cases, a person identified as a designated representative must be present to accept delivery of the classified material and sign the receipt; thereby accepting security responsibility.

(d) Delivery Outside the U.S., Its Territories, or Possessions:

1 Delivery Within the Recipient Country. U.S. Classified material to be delivered to a foreign government within the recipient country shall be delivered to a U.S. Government representative who shall arrange for its transfer to a designated representative of the recipient government. If the shipment is escorted by a U.S. Government official authorized to accomplish the transfer of custody, the material may be delivered directly to the recipient government's designated representative upon arrival.

2 Delivery Within a Third Country. Classified material to be delivered to a foreign government representative within a third country shall be delivered to an agency or installation of the U.S., or of the recipient government, that has extraterritorial status or otherwise is exempt from the jurisdiction of the third country. Unless the material is accompanied by a U.S. Government official authorized to accomplish the transfer of custody, a U.S. Government official shall be designated locally to receive the shipment upon arrival and be vested with authority to effect delivery to the intended recipient representative.

n. Overseas Carriers. U.S. classified material shall be transmitted outside the U.S. via ship, aircraft or other carriers that are:

(1) Owned or chartered by the U.S. Government or under U.S. registry; or

(2) Owned or chartered by or under the registry of the recipient government; or

(3) Otherwise expressly authorized by the head of the DoD component having classification jurisdiction over the material involved.

c. Freight Forwarders. Only freight forwarders that have been granted an appropriate FCL by DoD or the recipient government are eligible to receive, process, and store U.S. classified material authorized for release to foreign governments. However, a freight forwarder that does not have access to or custody of the classified material need not be cleared. *

18. Reproduction. All reproductions of classified material shall be marked or stamped with the same classification as the original. Only sufficient copies necessary to meet operational requirements shall be prepared, and reproductions shall be destroyed, if otherwise proper, as soon as they have served their purposes. Reproduction of classified material shall be made only on equipment specifically designated for the reproduction of classified material. Rules governing the use of such designated equipment will be conspicuously posted on or near the equipment. Further, appropriate warning notices prohibiting reproduction of classified material shall be posted on or near equipment used only for the reproduction of unclassified material.

a. Reproduction by Authorization Only. The contractor shall not make nor permit to be made without prior written authorization of the contracting officer, or his or her designated representative, any photograph or other reproduction of TOP SECRET information, SECRET information (when specifically prohibited), or CRYPTO information, regardless of classification, for any purpose. However, if the contract is for a TOP SECRET, SECRET, or CRYPTO report, then additional reproduction authority is not necessary. (See paragraph 87a regarding restrictions on the reproduction of COSMIC TOP SECRET information.) In addition, TOP SECRET and SECRET material originated by the DOE or its contractors may be reproduced only with the consent of the originator or higher authority within the responsible DOE activity.

b. Reproduction Not Requiring Authorization. The contractor may reproduce, without prior authorization of the contracting officer, non-CRYPTO information classified SECRET (unless specifically prohibited) or CONFIDENTIAL, when such reproduction is essential to the:

(1) performance of the contract,

(2) preparation of a solicited or unsolicited bid, quotation, or proposal to a UA of the U.S. Government or another authorized contractor for U.S. Government work,

(3) correspondence in connection with the contract, and

(4) preparation of patent application to be filed in the U.S. Patent Office. (This paragraph shall not be deemed to authorize the filing of patent applications, and such applications shall not be filed, except as specifically provided in the contract).

c. Records. The contractor shall maintain a record of the number of copies of all TOP SECRET, SECRET, and CRYPTO material, regardless of classification, that is reproduced. Reproduction records shall be retained by the contractor, for a minimum of 3 years for TOP SECRET, CRYPTO, or other special access material and for a minimum of 2 years for SECRET, and shall be incorporated in the control station records required by paragraph 12.

d. Additional Markings. When reproducing classified material, any additional marking shown on the original shall be shown on all reproductions.

19. Destruction.

a. Requirement for Destruction. The contractor shall establish a program for the review of classified material for the purpose of reducing to an absolute minimum the quantity on hand at any given time. With the exception of information listed in paragraph b below, contractors shall destroy classified material in their possession as soon as practical, after it has served the purpose for which it was:

(1) released by the government,

(2) developed or prepared by the contractor, and

(3) retained after completion or termination of the contract.

b. Disposition by Specific Authorization. COSMIC TOP SECRET material (see paragraph 85c(2)) shall not be destroyed, but shall be returned to the contracting officer or his or her designated representative. Accountable COMSEC classified material shall be destroyed only when destruction is authorized in writing by an appropriate government official. In all instances where specific instructions have been issued by the contracting officer, such instructions will dictate the disposition to be accomplished.

c. Methods of Destruction. Classified material 19/ shall be destroyed by burning or, with the written approval of the CSO, by shredding, pulping, melting, chemical decomposition, mutilation, or pulverizing (for example, hammer mills, choppers, and hybridized disintegrating equipment). The destruction process must be sufficient to preclude recognition or reconstruction of the classified information. The SPP shall include specific instructions which apply to the method of destruction, and shall incorporate instructions provided by the CSO. As applicable, the following additional requirements must be satisfied when classified material is destroyed.

(1) Public incinerators may be used only with the prior approval of, and under conditions prescribed by, the CSO.

(2) If the classified material is removed from the facility for destruction, it shall be destroyed on the same day it is removed.

(3) Ash residue produced by burning is to be examined and reduced by physical disturbance. If unburned material is found, the material shall be reprocessed for destruction.

(4) Only crosscut shredders producing residue particle size not exceeding 1/32 inch in width (with a 1/64 inch tolerance) by 1/2 inch in length, shall be used for destruction of classified paper and non-paper

---

19/ NATO Restricted information shall be destroyed by burning or other means approved for destruction of classified information.

products except microform material (see (7) below). Classified material shall be shredded in sufficient quantity and type of material to preclude reconstruction or recognition of the material being destroyed. When TOP SECRET material is shredded, a minimum of 20 pages of similar type, media, and print shall be destroyed at one time and the residue mixed in one container.

(5) Only paper-based products may be destroyed by pulping. High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellent type papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning shall be used to destroy these types of papers.

(6) When classified material is destroyed by either pulping or pulverizing, the equipment shall be equipped with security screens that do not exceed the following specifications:

(a) The security screen for pulping equipment shall have perforations of 1/4 inch or smaller.

(b) Security screens for pulverizers shall meet the following specifications:

1 shall not exceed 3/16 inch in diameter for hammer mills.

2 shall not exceed 3/32 inch in diameter for choppers and hybridized disintegrators.

(7) Classified material in microform: that is, microfilm, microfiche or similar high data density material shall be destroyed by burning, chemical decomposition or other methods as approved by the CSO.

(8) Procedures shall be established to ensure compliance with the manufacturer's instructions for operating the destruction equipment and to ensure its continuing effectiveness. These procedures shall include an inspection of the equipment after each time it is used to destroy classified material to assure effectiveness of the destruction process.

d. Witness to Destruction. The destruction of classified material shall be accomplished by, or in the presence of, two employees of the contractor who possess appropriate security clearances. One shall be a responsible employee who has been briefed in the destruction provisions of this paragraph, and who has been designated by the contractor to perform the destruction. The other shall be a responsible employee or a subcontract employee who is working on the premises of the contractor and who has been designated to witness the destruction of the classified material. However, CONFIDENTIAL material, other than accountable COMSEC material, may be destroyed at the facility and witnessed by: (i) one responsible employee, or (ii) one responsible subcontractor guard who is employed on a full-time basis at the facility, is under the supervision and direction of the FSO, possesses an appropriate PCL, has been briefed in the destruction procedures, and has been designated to perform and witness the destruction.

e. Destruction Records and Certificates for TOP SECRET, SECRET, or CRYPTO Material. When TOP SECRET, SECRET, or CRYPTO material, regardless of classification, is destroyed, the contractor, in addition to maintaining accountability records reflecting the destruction of such material, shall execute a destruction certificate indicating the date of destruction and identifying the material destroyed. The certificate shall be signed by both the individual designated to destroy and the individual designated as a witness at the time the material is destroyed. Both individuals shall be required to know, through their personal knowledge, that such material was destroyed. The contractor may, at his or her discretion, combine the information required in the destruction certificate with the accountability records maintained in accordance with paragraph 12a. On request, a copy of the destruction certificate shall be sent to the contracting officer at the time of destruction. Destruction records and destruction certificates shall be maintained at the control stations established under paragraph 12, and shall be retained by the contractor for a minimum of 3 years for TOP SECRET, special access, or CRYPTO material, regardless of classification, and for 2 years for SECRET material.

f. Classified Waste. Classified waste shall be destroyed as soon as practical, in accordance with the provisions of paragraph c above. This applies to all waste material containing classified information, such as preliminary drafts, carbon sheets, carbon ribbons, plates, stencils, masters, stenographic notes, worksheets, and similar items. Typewriter and ADP equipment ribbons used in transcribing classified material shall be safeguarded in the manner appropriate for the classification category involved, until the ribbon is cycled through the typewriter or printer a sufficient number of times to obliterate information contained thereon. Normally this can be accomplished if the ribbon is completely overprinted five times in all ribbon typing or printing positions. Any ribbon which remains substantially stationary (that is, receives at least five consecutive impressions) shall be treated as unclassified. CONFIDENTIAL waste, except waste containing CRYPTO or other special access information, may be destroyed by one employee or one responsible subcontractor guard pursuant to the provisions of paragraph d above. Pending destruction, classified waste shall be safeguarded in accordance with paragraph 14. Receptacles utilized to accumulate classified waste shall be clearly identified. Contractors shall develop procedures to ensure that accountable classified material is not inadvertently destroyed as classified waste. If not promptly destroyed, accountability shall be established over that material containing information classified SECRET or higher, special access information, or CRYPTO, regardless of classification, in accordance with paragraph 12f. When destruction does take place, the provisions of paragraph e above are applicable. * * *

g. Alternate Procedure. Where there is only one employee assigned at a facility and there is a need to destroy material, one or more of the following alternate procedures shall be used for disposal of the classified material:

(1) Return all classified material eligible for destruction, including classified waste, to the contractor or UA for whom the classified work is being performed, or to another facility of the same MFO.

(2) Utilize the destruction facilities of another DoD contractor or UA, provided that the individual granted use of such facilities retains physical custody of the classified material and personally ensures its complete destruction. To satisfy the requirements of paragraphs d and e above, an appropriately cleared employee of the contractor or UA providing the destruction service may serve as a witness to the destruction and sign the destruction certificate.

(3) Employ the destruction services of a subcontractor, vendor, or supplier specializing in the destruction of classified material, provided that the controls set forth in paragraph c above are observed and an appropriately cleared employee of another DoD contractor or UA is present to witness the destruction, when required pursuant to paragraph d and e above.

Section III. SECURITY CLEARANCES

20. General.

a. An individual shall be permitted to have access to classified information only when cleared by the U.S. Government or by the contractor, as specified in this section, and the contractor determines that access is necessary in the performance of tasks or services essential to the fulfillment of a contract or program; that is, the individual has a need-to-know. The contractor shall limit the number of personnel processed for a clearance to the maximum extent possible consistent with contractual obligations. The contractor must have a system, detailed in the SPP, for limiting personnel security clearances. The system must identify those required to make the deliberate decision as to a particular individual's need for a clearance and those who review the decision. The supervisor must certify that an employee will require access at a certain level of classification. Requests for a TOP SECRET clearance shall be reviewed for justification by designated official(s) at the executive management level and the personnel security application must be signed by the FSO or another cleared OODEP. The Secretary of Defense, through the Defense Investigative Service, reserves the right to limit the number of individual clearances issued to any cleared facility. The numbers and levels of security clearances possessed by a facility is regulated by a system administered by the CSO. Each contractor will be limited to a specific number of clearances consistent with the needs of the UA concerned.

b. Only U.S. citizens are eligible to be granted a standard PCL. * Under special circumstances and conditions, immigrant aliens and foreign * nationals may be authorized access to classified information at the SECRET * or CONFIDENTIAL level, with limitations, provided they are determined eligible * and have been granted a Limited Access Authorization (LAA). A U.S. * citizen must be 16 years old to be eligible for a CONFIDENTIAL clearance * and 18 years old to be eligible for a SECRET or TOP SECRET clearance. A * non-U.S. citizen must be 21 years old to be eligible for an LAA. *

c. A PCL granted by the DoD, or by a contractor as specified in this section, is valid for access on a need-to-know basis to all classified defense information at the same or lower category except for the following:

(1) Contractor-granted CONFIDENTIAL PCL's are not valid for access to classified foreign government information; RESTRICTED DATA; FORMERLY RESTRICTED DATA; COMSEC information (see DoD 5220.22-S); SENSITIVE COMPARTMENTED INFORMATION (SCI); ACDA classified information; * NATO information; to meet the PCL requirement as a prior condition for * certification to fill a Critical or Controlled Position under the Nuclear Weapon PRP; or for assignment to duty stations outside the U.S.

(2) Interim SECRET or interim CONFIDENTIAL PCL's are not valid for access to RESTRICTED DATA; FORMERLY RESTRICTED DATA; NATO; COMSEC; and SCI.

(3) Interim TOP SECRET PCL's are valid for access to RESTRICTED DATA; FORMERLY RESTRICTED DATA; NATO; COMSEC; and SCI only at the SECRET level and below.

(4) Access by foreign nationals and immigrant aliens under an LAA is limited as set forth in paragraph 31.3 and by the terms under which each LAA is granted.

d. Personnel shall not be cleared for access to classified information of a higher level than the clearance of the facility at which they are employed except for: (i) Type A Consultants whose services are being utilized by another contractor or a UA; and (ii) certain cleared employees of an MFO who are employed or physically located at a subordinate facility with a lower level of clearance or at an uncleared facility within the MFO.

e. A personnel security clearance is neither a license for access to classified information, nor a substitute for security measures designed to prevent unauthorized access. Therefore, security clearances under the DISP are to be granted only when there is a bona fide requirement for access to classified information in performance of duty assignment, and when otherwise required by the terms of this manual.

f. The fact that a contractor has qualified for and has been granted an FCL shall not be used for advertising, promotional purposes, or in the recruitment of employees. Employment advertisements shall neither state nor imply that a PCL is a condition or prerequisite for employment. Reproduction in any manner of the "Letter of Notification of Facility Security Clearance" (DIS FL 381-R), furnished to the contractor by the U.S. Government, shall not be made except for the necessary records of the contractor or unless requested by a competent U.S. Government authority. Further, the reproduction in any manner of a DISCO Form 560 (Letter of Consent (LOC)) furnished by the government to the contractor shall not be made, except for necessary records of the contractor, or unless requested by competent U.S. Government authority. A copy of the LOC shall not be furnished the employee named on the form for any purpose whatsoever, nor shall the employee be given any other written notification of the granting of a clearance or access authorization. However, this does not preclude the issuance of a color-coded identification card or badge to reflect the level of access authorized pursuant to paragraph 8.

g. When determined that full investigative coverage or other required assurances cannot be satisfied for the level of PCL or LAA requested, the contractor shall be so advised by DISCO and all related investigative action will be discontinued.

h. Unless administratively terminated, suspended, or revoked by the DoD, the LOC for an employee remains effective so long as he or she is continuously employed by the contractor. If the employee no longer requires access to classified information and no bona fide need for such access is anticipated within the next 120 days, the PCL shall be administratively terminated. In addition, if an employee has been placed in layoff status or is granted a temporary leave of absence for 120 days or less, it shall not be considered as an interruption or discontinuance of employment. If the employee does not return to active employment within 120 days, he or she shall be reported terminated, effective the first day of the absentee period.

i. In all cases in which a contractor furnishes copies of board minutes, certificates, or other records, such records shall be on company letterhead or identified by typing the contractor's name and address and reflect the date of submission.

j. As a general rule, a contractor may be issued only one LOC for each cleared employee. However, in the case of an individual who is required to be cleared in connection with the HOF FCL and who has his or her primary place of work at another facility of the MFO, an LOC may be issued to both facilities.

k. Requests for PCL's for employees who are RFI's shall be submitted to DISCO. RFI's are not eligible for PCL's if: * *

(1) the foreign interest involves a "Designated country" or a citizen, firm, or other entity of a "Designated country"; or

(2) their work as RFI's could create a potential conflict of interest situation vis-a-vis their work for the contractor. By way of example, a potential conflict of interest situation is considered to exist when an individual represents a foreign government, or is in the employ of a foreign government, or an individual's technical or scientific endeavors on behalf of a foreign interest are similar to his or her technical or scientific endeavors on behalf of the U.S. contractor; or

(3) they are not U.S. citizens or U.S. nationals.

Decisions as to whether an individual is eligible for a PCL pursuant to paragraph (1), (2), or (3) above are made by DIS. With the exception of the foregoing, RFI's are eligible for consideration for PCL's provided they submit statements explaining fully their foreign connections. The statement shall identify the foreign entity. If it is a business enterprise, the statement shall explain the nature of the business and to the extent possible, details as to its ownership, including the citizenship of the principal owners or blocks of owners. The statement shall fully explain the nature of the relationship between the applicant and the foreign entity and indicate the approximate percentage of the applicant's time devoted to the interest of the foreign entity. In addition, the statement shall incorporate the provision that the applicant recognizes his or her special responsibility to protect classified information from disclosure to any unauthorized person, foreign or domestic. Two copies of the statement described above shall be included with each request for an initial PCL, transfer or reinstatement of PCL, concurrent PCL, or conversion of clearance. In those cases where an employee who is cleared (or is in the process of being cleared) becomes an RFI, the contractor shall submit a written report which shall include the statement described above. In those cases where an RFI is required to be cleared in connection with an FCL, the provisions of paragraph 22f also apply.

l. Persons not eligible for a PCL under the provisions of this section may be granted access to classified information only as specifically authorized in writing by a UA. The granting of such access is beyond the scope of the DoD Industrial Security Program, and all necessary instructions will be provided by the UA concerned.

m. When an interim PCL has been granted and derogatory information is subsequently developed, DISCO may withdraw the interim PCL pending completion of the processing which is a prerequisite to the issuance of a final PCL. When an interim PCL for an individual who is required to be cleared in connection with the FCL is withdrawn, the interim FCL will also be withdrawn unless action is taken to remove the individual from the position requiring a PCL. Withdrawal action is not a denial or revocation of a PCL and is not appealable.

n. Periodically, the need arises for DISCO to reconcile its personnel security clearance records with those of the contractor. When furnished with a list of cleared personnel by DISCO, the contractor shall annotate the listing with any corrections or adjustments and return it at the earliest practical time. The reply shall include a statement by the facility FSO certifying whether the individuals listed remain employed in positions requiring access to classified information.

20.1. Emergency Higher Level Access. Contractors may experience circumstances where an urgent operational need or a contractual exigency exists for one or more of its employees to have one-time or short duration access to classified information at a higher level than is authorized by the pertinent PCL in effect. In many instances, the processing time required to upgrade the PCL would preclude timely access to the information. In such situations, and only for compelling reasons [1] in support of the national interest, contractors are authorized to grant higher level access on a temporary basis subject to advance approval (verbal, if necessary, but later confirmed in writing) from the CSO and adherence to the terms and conditions prescribed below. This authority may be revoked by the CSO for abuse, inadequate record keeping, or improper security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level PCL. Additional procedures and conditions for effecting emergency access to information at a classification level above that reflected on a current LOC are as follows:

a. The employee must be a U.S. citizen and possess a current government-granted clearance. The access required shall be limited to classified information one level higher than the classification level reflected on the LOC in effect.

b. Justification for the higher level access shall be approved, in writing, by the facility FSO or his or her single designee for this purpose. Emergency access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the CSO.

---

[1] A "compelling reason" as used herein, is expressly limited to circumstances concerning a paramount matter that would permit the avoidance of an unacceptable delay in contract performance, precontract activity or in special cases to overcome a critical technical or engineering problem, the time-sensitive solution to which is deemed essential to fulfill a crucial contract performance criterion.

c. The employee to be afforded the higher level access shall have been continuously employed by the contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees or consultants for any period of time without the written approval of the UA contracting officer concerned.

d. Pertinent facility records concerning the affected employee shall be reviewed and no significant adverse information concerning that person shall be known to the contractor, that is, adverse information reportable pursuant to paragraph 6b(1).

e. Access shall be confined to a single instance or a few occasions. The duration of access shall not normally extend beyond 30 calendar days from date of access inception. If the need for access is expected to continue for a period in excess of 30 days, written authority of the UA contracting officer is required. If the need for access is expected to extend beyond 90 days, the facility shall promptly place the affected employee in process for the higher level PCL concurrent with the granting of emergency access. When extended access is approved by the UA, such access shall be canceled at or before 90 days from the original date of access inception. The exercise of emergency access shall be used sparingly, and repeat use of this unique arrangement within any 12-month period on behalf of the same individual is prohibited.

f. Access at the higher level shall be limited to information under the control and custody of the authorizing contractor and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for recording the higher-level information actually revealed along with each date such access is afforded, and for daily termination of higher-level access and retrieval of pertinent material for proper safekeeping.

g. Access at the next higher level shall not be authorized for COMSEC, SCI, NATO, RESTRICTED DATA or foreign government information. *

h. The contractor shall document the need for affording the employee a higher-level access and maintain all related documentation for 5 years. A copy of the documentation shall be forwarded to the CSO and the UA concerned. As a minimum, this documentation shall include:

(1) The name and social security number of the employee afforded higher level access and the level of access authorized.

(2) Justification for the access, to include a full explanation of the compelling reason to grant the higher level access and precisely how the national interest would be served to do so. This justification shall include the signature of the FSO and the name of the CSO official who approved access and the date thereof.

(3) An unclassified description of the specific information to which access was authorized and granted, and the duration of access along with the date(s) access was afforded.

(4) A listing of the facility records reviewed and a statement that no adverse information concerning the employee is known to the contractor.

(5) Copies of any pertinent briefings/debriefings administered to the employee.

21. Facility Security Clearances.

a. Procedures for Processing. An FCL is an administrative determination that a facility is eligible from a security viewpoint for access to classified information of the same or lower classification level as the clearance being granted. FCL's shall not be granted to contractor activities located outside the U.S., Puerto Rico, or a U.S. possession or trust territory. FCL's may be granted only to contractors organized and existing under the laws of any of the fifty states and Puerto Rico. Contractors organized and existing under the laws of a U.S. possession or trust territory may not be processed for or granted an FCL unless prior approval is received from the Deputy Director (Industrial Security), HQ DIS. The CSO assigned responsibility for the geographic area in which the facility is located (see appendix VIII) will advise the prospective contractor of the actions required for the processing, the issuance, and the continuation of an FCL. In connection with the issuance of an FCL, PCL's must be granted to certain management personnel as prescribed in paragraph 22. In addition, the contractor shall execute a "Department of Defense Security Agreement" (DD Form 441); or, where appropriate, an "Appendage to Department of Defense Security Agreement" (DD Form 441-1) and a "Certificate Pertaining to Foreign Interests" (DD Form 441s). In the case of an MFO, where more than one facility is covered by the DD Form 441 or DD Form 441-1, the contractor shall furnish a copy of the DD Form 441 with DD Form 441-1, when appropriate, to each facility covered under the agreement and to the CSO of each covered facility. Before a contractor is eligible for custody of classified information, the contractor, in addition to having an FCL, shall have appropriate and CSO approved storage capability and be prepared to apply such other safeguards as prescribed by this manual. Classified information which is of a higher security classification than the contractor's FCL shall not be disclosed to the contractor. *

b. Licensing, Patent, and Trade Secret Agreements. Licensing, patent, and trade secret agreements with a foreign entity may render a contractor ineligible for an FCL, unless appropriate procedures are established in the facility's SPP to ensure that such agreements will not jeopardize the security of classified information, which is entrusted to the contractor. In this connection, attention is directed to the State Department's ITAR, in particular, parts 124 and 125 thereof. This regulation provides, inter alia, that before the execution of any license agreement envisaging the transmittal abroad of classified U.S. military information, it must first be submitted to the Department of State for review and approval, and that prior to any approval of such agreement, the release of the classified information involved must be approved by the cognizant U.S. military department and the DoD under established procedures.

c. Foreign Ownership, Control, or Influence (FOCI). Except as provided for elsewhere in this manual facilities which are determined to be under FOCI are not eligible for an FCL. Agreements with a foreign interest may make a contractor ineligible for an FCL. Execution of a DD Form 441s (see appendix I, paragraph M) is required in connection with a determination of the degree, if any, of FOCI. The contractor must execute a new DD Form 441s whenever there is any change in the information previously submitted (it is not necessary to repeat answers on the new DD Form 441s which have not changed). In addition, when any question on the DD Form 441s has been answered affirmatively, a new complete DD Form 441s must be submitted every 5 years from the date of the last change submitted. If no changes have occurred, a statement to this effect is necessary. Any investor who has acquired a direct or indirect beneficial ownership interest of 5 percent or more of any class of stock of a registered company, or any investor who plans to make a tender offer to purchase securities, which is reasonably expected to result in such an ownership interest, is required to file a Schedule 13D report with the SEC, with the company whose securities are involved, and with any national exchange on which the securities may be traded. If the acquisition will result in the submission of a revised DD Form 441s, and the contractor has received Schedule 13D from the investor, a copy of the Schedule 13D will be forwarded with the DD Form 441s or, if appropriate, with the report (notification letter) required by paragraph 6a(4)(f). A new DD Form 441s shall also be executed by the contractor whenever advised that the form is required for an official purpose. It is the contractor's responsibility to provide complete information to ensure that the degree of FOCI to which the facility may be subjected is fully explained to enable the U.S. Government to ascertain whether classified information entrusted to the contractor is, or could be, jeopardized.

d. Sponsorship of Freight Forwarders for a Facility Clearance

(1) A foreign embassy normally serves as sponsor for a freight forwarder and is responsible for initiating the request for the FCL. The request shall indicate the level of secure storage required. Freight forwarders are not authorized to transmit TOP SECRET material. This request shall be sent to Defense Logistics Standard Systems Office (DLSSO), 6301 Little River Turnpike, Alexandria, Virginia 22312-5044 for inclusion in the MAPAD. The embassy request must also designate the freight forwarder as its agent and specify that the firm will assume full security responsibility for the material on behalf of the foreign government. After receipt of the clearance request, DLSSO will forward the request to Headquarters, DIS, Attn: Deputy Director (Industrial Security).

(2) User Agencies and contractors may request an FCL for freight forwarders who process U.S. classified material for overseas shipment to U.S. locations. The request shall be submitted to Headquarters, DIS, ATTN: Deputy Director (Industrial Security).

(3) User Agencies who receive clearance requests for freight forwarders on behalf of foreign governments to process foreign military sales (FMS) shall advise the governments of the provisions of subparagraph d(1) above.

(4) If a foreign government requires a shipping office at a freight forwarder location, the freight forwarder must have an FCL. The foreign government must submit a clearance request in accordance with subparagraph d(1) above. * * * *

22. Personnel Clearances Required in Connection with Facility Clearances. Certain individuals, as described below, must be processed for a clearance in connection with FCL's. Unless notified by the CSO that such determinations are not required, individuals other than those described below, who exercise control over the management of the facility through stock ownership, proxy voting rights, majority ownership of securities, or by some other method control the management of the facility and affect the appointment and tenure of officers, directors, or principal supervisory management personnel of the facility, shall be processed for a determination of clearance eligibility by the CSO in connection with the FCL.

a. Corporations, Associations, and Nonprofit Organizations. Except as provided for below, the following individuals are required to be cleared in connection with, and at the level of, the FCL.

(1) The chairman of the board and all principal officers.

(a) Other officers [2], who shall not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared, provided the organization complies with the provisions of paragraph e below (exclusion action is not required for assistant secretaries, assistant treasurers, and assistant vice presidents who do not have management responsibilities related to performance on classified contractors); or

(b) Other officers who require access to classified information in the conduct of the organization's business, but at a lower level than that of the FCL, may be cleared with a U.S. Government granted PCL at the lower level, provided they do not occupy positions that would enable them to affect adversely the organization's policies and practices in the performance of the higher level classified contracts, and the organization complies with the provisions of paragraph e below.

(2) Directors who require access to classified information must be cleared. Directors who do not require access to classified information in the conduct of the organization's business, and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not

---

[2] All officers, as defined by paragraph 3bj, are considered OODEPs of an organization, but not all OODEPs occupy positions required to be cleared in connection with an FCL.

required to be cleared. A director who also serves as a principal officer shall be cleared. If the corporation or association conducts meetings with a pro tem chairman or by a rotating chairmanship, all board members who are eligible for or who could sit as board chairman shall be cleared, and, with respect to all uncleared directors, the organization shall comply with the provisions of paragraph e below. If the board has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, only the members of this committee who require access to classified information shall be cleared. Other directors shall be excluded in accordance with the provisions of paragraph e below. Two copies of the instrument establishing the executive committee shall be furnished to the CSO.

(3) The management official in charge at the facility and the FSO.

(4) A current list of all OODEPs shall be maintained by the facility, with a copy furnished to the CSO. The list shall designate by name those individuals granted an LOC, those who are being processed for a PCL, and those who have been excluded from access to classified information pursuant to the provisions of paragraph e below. Such lists shall be signed by an OODEP of the corporation.

b. Sole Proprietorships. The following individuals are required to be cleared in connection with, and at the level of, the FCL:

(1) The owner must be cleared.

(2) All officers, if applicable, must be cleared.

(3) The management official in charge of the facility and the FSO.

(4) A current list of all OODEPs shall be maintained by the sole proprietorship and the CSO. The list shall designate by name those individuals granted an LOC, those who are being processed for a PCL, and those who have been excluded from access to classified information pursuant to the provisions of paragraph e below. Such lists shall be signed by an OODEP of the sole proprietorship.

c. Partnerships. Except as provided for below, the following individuals are required to be cleared in connection with, and at the level of, the FCL:

(1) General partners must be cleared.

(2) All other partners:

(a) Partners, other than general partners, who do not require access to classified information in the conduct of the organization's business and do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared and the organization by official action of the general partners shall comply with the provisions of paragraph e below. or

(b) Partners, other than general partners, who require access to classified information in the conduct of the organization's business, but at a lower level than that of the FCL, shall be cleared at the lower level provided they do not occupy positions that would enable them to affect adversely the organization's policies and practices in the performance of higher-level classified contracts, and the partnership, by official action of the general partners, complies with the provisions of paragraph e below.

(3) If the partnership has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, all members of this committee shall be cleared in connection with the FCL. Other nonexecutive committee member general partners shall be excluded, provided the committee has full executive authority to exercise management control and supervision for the partnership, and, with respect to these other partners, the organization complies with the provisions of paragraph e below. Two copies of the partnership's resolution delegating this authority to the committee shall be furnished to the CSO. The resolution shall specify which partners are excluded from access to all classified information, and which partners are excluded from access to higher-level classified information, as appropriate.

(4) The management official in charge of the facility and the FSO.

(5) A current list of all OODEPs shall be maintained by the partnership, with a copy furnished to the CSO. The list shall designate by name those individuals granted an LOC, those who are being processed for a PCL, and those who have been excluded from access to classified information, pursuant to the provisions of paragraph e below. Such lists shall be signed by an OODEP.

d. Colleges and Universities. Except as provided for below, the following individuals are required to be cleared in connection with, and at the level of, the FCL:

(1) The chief executive officer.

(2) Those other officers or officials who are specifically and properly designated by action of the board of regents, board of trustees, board of directors, or similar executive body, in accordance with the institution's requirement, as the managerial group having the authority and responsibility for the negotiation, execution, and administration of UA contracts, shall be cleared. The institution shall furnish the CSO a copy of such designation of authority, from which the particular officers who are to be processed in connection with an FCL can be determined, and thereafter, changes shall be furnished as they occur. If this requirement is not met, all officers shall be processed for PCL's in connection with the FCL.

(3) Regents, trustees, or directors:

(a) Regents, trustees, or directors who shall not require access to classified information in the conduct of the institution's business and who do not occupy positions that would enable them to affect adversely the institution's policies or practices in the performance of classified contracts shall be excluded. If the college or university conducts meetings with a pro tem chairman or by a rotating chairmanship, all board members who are eligible for, or could sit as, board chairman shall be cleared. With respect to all uncleared regents, trustees, or directors, the institution shall comply with the provisions of paragraph e below.

(b) If the board has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee or managerial group, only the members of this committee or group who require access to classified information shall be cleared. Other regents, trustees, or directors shall be excluded in accordance with the provisions of paragraph e below. Two copies of the instrument establishing the executive committee shall be furnished to the CSO.

(4) The management official in charge of the facility and the FSO.

(5) A list of OODEPs shall be maintained by the college or university with a copy furnished to the CSO. The list shall designate by name those individuals granted LOC's, those who are being processed for PCL's, and those who have been excluded from access to classified information, pursuant to the provisions of paragraph e below. Such lists shall be signed by an OODEP of the college or university.

e. Exclusion Procedures. This paragraph applies to those officers, directors, partners, regents, and trustees who can be excluded altogether from the requirement for a PCL, or who can be excluded from higher-level access by virtue of possessing a PCL at a level below that of the FCL. The organization by formal action of the board of directors, all general partners, or similar executive body, shall affirm the following, as appropriate.

(1) Such officers, directors, partners, regents, or trustees (designated by name) shall not require, shall not have, and can be effectively excluded from access to all classified information in the possession of the organization. They also do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts or programs. This action shall be made a matter of record in the organization's minutes of the board of directors, partnership, board of regents, or trustees, or similar executive body. Two copies of such minutes, dated and identified by the name and address of the facility, shall be furnished to the CSO.

(2) Such officers or partners (designated by name) shall not require, shall not have, and can be effectively denied access to higher-level classified information (specify which higher level(s)) and do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of higher-level classified contracts (specify higher level(s)) or programs for the UA's. This action shall be made

a matter of record in the organization's minutes of the board of directors, partnership, board of regents, or trustees, or similar executive body. Two copies of such minutes, dated and identified by the name and address of the facility, shall be furnished to the CSO.

f. Representative of a Foreign Interest. When an RFI is required to be cleared in connection with an FCL, and the RFI has not been excluded in accordance with paragraph e above, the following procedures shall apply:

(1) When the statement required by paragraph 20k has been executed, official notice of its execution shall be made a matter of record in the organization's minutes by the board of directors or similar executive body. Two copies of the minutes shall be furnished the CSO.

(2) Failure to obtain a PCL for, or to exclude an RFI, shall make the facility ineligible for clearance and any existing FCL shall be administratively terminated by the CSO. Such action is not appealable.

(3) In those cases where an individual who is cleared in connection with the FCL becomes an RFI, the contractor shall submit the report required by paragraph 6a(4)(d), in addition to the actions prescribed in this paragraph.

g. Special Procedures For Clearing Freight Forwarders. Only the chief executive officer, FSO, and shift supervisors are required to be cleared. Supervisors are responsible for the protection of classified material when moved from a storage area to a mode of transportation. Other individual(s) who require unsupervised custody of classified shipments shall be cleared. An individual moving classified freight under the supervision of a cleared supervisor need not be cleared. Freight forwarders are only authorized to move classified freight to the country for which the freight forwarder serves as agent.

23. Security Clearance of Negotiators. Negotiators designated by the contractor as being required to participate in the preparation of a bid or quotation may be processed for PCL's concurrent with, but not as a part of, the FCL. An FCL is not dependent on the granting of a PCL to negotiators, and changes in negotiators shall not affect the status of an FCL.

24. Security Clearance of Additional Personnel. Except in the case of personnel who are required to be cleared in connection with an FCL, and negotiators, the contractor shall not initiate PCL action on employees until an FCL has been granted. Contractor employees, other than those cleared in accordance with the provisions of paragraphs 22, 23, 27, or 31, whose access to classified information is essential in the performance of a classified contract, shall be cleared as specified below.

a. Clearance by the DoD.

(1) DoD shall grant PCL's for U.S. citizen employees of the contractor who:

(a) require access to information classified TOP SECRET 3/ or SECRET, or to any COMSEC information, regardless of classification, SENSITIVE COMPARTMENTED INFORMATION, RESTRICTED DATA or FORMERLY RESTRICTED DATA, and classified foreign government information;

(b) are employed by a college or university;

(c) require access to NATO information classified CONFIDENTIAL or higher as described in section XI;

(d) require access to ACDA classified information;

(e) make determinations to grant access authorizations, in accordance with paragraph b below;

(f) are RFI's;

(g) require security clearances as a condition of the Nuclear Weapon PRP for duties in Critical and Controlled positions under the Nuclear Weapon Security Program (see paragraph 3b1); or

(h) are employed by a freight forwarder. *

(2) DoD shall grant PCL's for employees of contractors whose applications for clearances are required to be referred to DISCO, pursuant to paragraph b below.

(3) DoD shall grant Limited Access Authorizations (LAA's) for non-U.S. citizen employees of the contractor who require access to classified information (see paragraph 31).

b. Clearance by the Contractor. Contractors are delegated authority to act for and on behalf of the DoD to grant clearances at the CONFIDENTIAL level to qualified U.S. citizen employees who have a fully justified and bona fide requirement for access to CONFIDENTIAL information. Contractors shall not grant CONFIDENTIAL clearances to employees for any other purpose. CONFIDENTIAL clearances granted by the contractor shall remain valid, unless otherwise revoked by the DoD, within any facility of the same organization, so long as the individual continues in the contractor's employment. A contractor is not authorized to revoke such a clearance. However, if the employee no longer has or requires access to classified information in the foreseeable future, the clearance shall be administratively terminated in accordance with paragraph 29. The contractor is not authorized to grant an interim CONFIDENTIAL clearance. Contractor-granted CONFIDENTIAL clearances are not valid for access to RESTRICTED DATA; FORMERLY RESTRICTED DATA; any COMSEC information; SENSITIVE COMPARTMENTED INFORMATION; ACDA classified information; NATO information; to meet the PCL requirement as a prior

---

3/ When a TOP SECRET clearance is requested, DISCO will automatically issue an LOC for SECRET when the investigation necessary for a PCL at the SECRET level has been completed with satisfactory results. That LOC will subsequently be superseded by an LOC for TOP SECRET when the required additional investigation is completed.

condition for certification to fill a Critical or Controlled Position under the Nuclear Weapon Security Program; classified foreign government information; or for assignment to duty stations outside the U.S. Moreover, contractor-granted CONFIDENTIAL clearances granted to employees who are subsequently assigned to duty stations outside the U.S. shall be administratively terminated.

(1) A contractor is authorized to grant a CONFIDENTIAL clearance to a U.S. citizen employee provided the contractor makes a determination of trustworthiness prior to granting the clearance and access is essential to the accomplishment of lawful and authorized Government purposes. The contractor shall make the determination of trustworthiness based on a favorable review of the following:

(a) Personnel records and related screening procedures used to evaluate initial and continuing eligibility and suitability for employment and all of the records maintained on the employee that might be materially significant to PCL consideration. As a minimum, verification of prior employment and contact with listed references shall be accomplished.

(b) The "Application and Authorization for Access to Confidential Information (Industrial)," DD Form 48-2, executed by the employee indicates that: (i) the employee is a U.S. citizen; (ii) the employee is not an RFI; (iii) the information furnished in item 4 of the form, if any, does not reflect that a PCL has been suspended, denied, or revoked; and (iv) the certification section of the form has been signed and witnessed. * * *

(c) Documents indicating that the individual is a U.S. citizen. Verification of U.S. citizenship shall be accomplished by the contractor by sighting documents described in appendix XII. If the required documentary evidence is not immediately obtainable, the contractor may grant the CONFIDENTIAL clearance after having explained to the employee that the clearance is conditional, based on submission of the necessary documentary evidence as soon as possible, but, in any event, no later than 90 days. If the employee does not produce the necessary proof of U.S. citizenship within 90 days, the contractor shall administratively terminate the CONFIDENTIAL clearance which may be reinstated immediately upon presentation of proof of citizenship.

(2) When the contractor is satisfied with the trustworthiness of the employee, the contractor, acting for and on behalf of the DoD, is authorized to complete Part II of the DD Form 48-2 indicating that the employee is granted a clearance for access to CONFIDENTIAL information. * * * *

(3) If an employee indicates in item 3 of the DD Form 48-2 of having applied for or having received a previous PCL but gives no indication in item 4 of the form that a prior PCL has ever been suspended, denied, or revoked, the contractor is authorized to make a favorable determination, if otherwise appropriate. However, a copy of the DD Form 48-2 shall be sent to DISCO for a check of the PSCF. * *

(4) When circumstances are such that the contractor is unable to *
make the required determination of trustworthiness or because the employee *
(i) indicates that access or a clearance was denied, revoked or suspended; *
(ii) lists residence in a Designated country within the past 15 years under *
Item 10; (iii) lists relatives living in Designated countries under item *
11; or, (iv) indicates being an RFI under item 12, the contractor shall not
grant the employee a clearance for access to CONFIDENTIAL information.
Instead, the contractor shall submit to DISCO one copy of the completed Part
I of the DD Form 48-2 together with the forms prescribed in paragraph 26b,
for further evaluation and determination of eligibility for a security
clearance for access to CONFIDENTIAL information. The contractor shall
include a statement explaining the basis for referral.

(5) In the event the employee refuses to complete the certification portion of the DD Form 48-2 by signature as required, the form will be considered incomplete and the contractor shall not grant the clearance or access to classified information pending completion of the form.

(6) The authority to grant clearances at the CONFIDENTIAL level may be rescinded by the CSO if abuse becomes evident or if the contractor is unable to comply with the provisions set forth above. When such occurs, the contractor shall be required to submit requests for such clearances to DISCO in accordance with paragraph 26b. The privilege may be restored by the CSO only upon a showing of good cause.

(7) Freight forwarders processed under paragraph 22g are pro- *
hibited from issuing contractor-granted CONFIDENTIAL clearances. *

25. Preemployment Clearance Action. The contractor shall not initiate any *
preemployment clearance action except as provided for in this paragraph. *
An applicant for employment in a position that requires access to *
classified information may be informed that a PCL will be required. A *
personnel security questionnaire (PSQ) may be given to such an individual *
being considered for employment, but the contractor shall not obtain or *
review the completed form until after the individual is employed and placed *
on the payroll. However, in exceptional cases the completed application *
forms may be obtained and submitted to DISCO prior to the date of entry on
duty. The exception is limited to cases in which a written contract for
future employment has been executed between the prospective employee and the
employer that prescribes a fixed date for entry on the payroll, normally not
to exceed 120 days from the effective date of the employment contract.

26. Application for Personnel Security Clearance.

a. General.

(1) Contractors shall make application for DoD PCL's in *
accordance with the provisions of this section. Applications for all PCL's *
shall be mailed to DISCO, P.O. Box 2499, Columbus, Ohio 43216 or shall be *
electronically transmitted in accordance with appendix XVI. For PCL's *
required in connection with an FCL, applications shall be marked "OODEP" *
where contract number is requested. In addition to the forms and related *
documentation required in connection with the application for a PCL, the *
contractor shall compile and submit other information when requested by *
DISCO or the CSO to satisfy an official U.S. Government requirement. *

Failure by any employee to furnish PCL application forms, when requested or when required by this manual, shall preclude the granting of any new PCL to the applicant, and shall constitute sufficient basis for the DoD to administratively suspend any outstanding PCL of the employee concerned and discontinue all processing action. Resumption of case processing will only be approved upon showing of good cause by the applicant. Whenever a contractor employee has submitted forms prescribed by this paragraph to DISCO but subsequently objects, for any reason, to being processed for a PCL or to have an existing PCL continued, the contractor shall report all relevant facts to DISCO. Verification of such objections shall be made by the U.S. Government. On verification, any pending PCL processing action shall be discontinued, and any PCL then held by the employee shall be administratively terminated by the U.S. Government without prejudice to the employee.

(2) The DD Form 48, DD Form 49 and DD Form 48-3 shall be completed *
jointly by the employee and the contractor, however, the information *
required by the PSQ is intended to serve a specific and authorized government *
purpose; namely, to assist the DoD in determining the eligibility of *
an applicant for a PCL pursuant to the requirements of this Manual. Contractors *
are prohibited from using such information for other than its *
intended purpose. Contractors shall establish procedures for completing *
the PSQ's as follows: *

(a) When providing an employee with a PSQ, the contractor shall inform the employee that information concerning the Privacy Section and preaddressed envelopes no longer applies.

(b) Each employee shall be advised that if they believe there is a significant personal matter which they desire not to disclose to their employer, they may request an interview with a DIS agent by entering "DIS Interview Requested" rather than completing the specific item.

(3) The employee shall be further advised that on completion *
of the PSQ, it shall be returned to the contractor for review and mailing. *
The contractor shall review the PSQ to determine its adequacy and to *
ensure that necessary information has not been omitted before forwarding *
it together with the "Applicant Fingerprint Card (FD Form 258), to DISCO. *
(The FD Form 258 is not required when a DD Form 48-2 or DD Form 48-3 is *
submitted. It is required in connection with all other submissions.) *

(4) The employer shall ensure that the "Applicant Fingerprint *
Card," if required, is properly completed. In addition, the contractor *
shall establish procedures to ensure that an employee of the contractor *
will witness the taking of the employee's fingerprints on the card to *
ensure that the person fingerprinted is, in fact, the same as the employee *
being processed for the clearance. *

(5) The completed personnel security forms shall be forwarded to *
DISCO.

(6) All forms required by this section, may be obtained from *
DISCO. Instructions for completion of such forms are contained in pamphlets *
which are also available from DISCO. These pamphlets are entitled: *
(i) "Detailed Instructions for Completion of DD Form 48, Personnel Security *

Questionnaire (Industrial - NAC)," (ii) "Detailed Instructions for Completion of DD Form 49, Personnel Security Questionnaire Industrial (BI/SBI)," and (iii) "Instructions for Competion of DD Form 48-3." * * *

b. New clearances. Application for an initial PCL, for upgrading an existing PCL, or for requesting a PCL in situations where other provisions of this manual are not applicable, shall be made by the contractor by submission of the following forms:

(1) DD Form 48 4/, completed and executed by U.S. citizens who are to be processed for a DoD issued CONFIDENTIAL or SECRET clearance unless paragraph (2) below applies;

(2) DD Form 49 5/, completed and executed in the following cases:

(a) U.S. citizens who are to be processed for TOP SECRET clearance,

(b) U.S. citizens who are to be processed for any level of PCL when the applicant lists relatives or relatives of his or her spouse who are residing in Designated countries,

(c) U.S. citizens who are to be processed for any level of clearance when the applicant advises he or she is an RFI, and

(d) immigrant aliens and foreign nationals who are to be processed for a SECRET or CONFIDENTIAL LAA.

(3) A properly completed and executed FD Form 258 with each request submitted pursuant to paragraphs (1) or (2) above. Care shall be exercised to ensure that fingerprints are authentic, legible, and complete. Those which do not meet prescribed standards shall be returned for reexecution, which will result in clearance delays. The employee shall deliver the completed forms to the designated company representative who will ensure mailing.

c. Interim Clearances. Except as authorized below, requests for an interim TOP SECRET PCL shall be forwarded to the contracting officer for approval by the head of the contracting activity or his or her designated representative. Approval will be given only in an emergency situation in order to avoid crucial delays in precontract negotiation, or in the award or performance on a contract. The contractor shall: (i) obtain

---

4/ The DD Form 48 packet consists of an original and 1 copy of the PSQ.

5/ The DD Form 49 packet consists of two sections: section I -- a DD Form 49 worksheet printed on the reverse of the instructions, and the DD Form 49 packaged as a 5-copy carbon set; and section II -- a DD Form 2221, and an original and one copy of a privacy section.

such approval and submit it with the application for the interim TOP SECRET PCL, or (ii) forward the application for interim TOP SECRET PCL through the contracting officer. The words "Interim TOP SECRET" shall be placed in bold letters in the lower right-hand corner of the "Job Title" block of the DD Form 49. The approval letter from the contracting officer shall be attached behind the FD Form 258. As an exception to the foregoing procedures, when an emergency situation exists which would render the facility incapable of adequately safeguarding classified material in its possession and no contracting officer is available to approve the interim TOP SECRET PCL request within the time required to negate the threat, the CSO is authorized to approve such requests prior to dispatch of the pertinent forms to DISCO. There is no need to pursue interim clearance action below the TOP SECRET level. Applicants for SECRET and CONFIDENTIAL PCL's will be summarily granted interim SECRET or interim CONFIDENTIAL PCL's, as appropriate, provided initial investigative coverage fails to uncover adverse information of material significance. If results are favorable following completion of full investigative requirements, a subsequent LOC will be issued by DISCO to remove the interim status of the outstanding PCL. Access limitations for interim PCL's are set forth in paragraph 20c(ii) and (iii). Interim action for non-U.S. citizen employees under consideration for an LAA is not authorized. *

d. Clearance Transfers and Reemployments.

(1) Application for a PCL may be made by the contractor for whom an LOC was previously issued while the individual was employed by the contractor or another contractor, provided not more than 24 months has elapsed since termination of the employment for which the LOC was issued. Application shall be made by submitting a DD Form 48-3 to DISCO. DISCO will issue a new LOC for the employee. When more than 24 months has elapsed since termination of the PCL, the contractor shall make application for clearance using the procedures required for new clearance actions (paragraph 26(b)). *

(2) Contractor-granted CONFIDENTIAL clearances may not be transferred from one facility to another except in the case of an MFO as provided for in paragraph e below. Application for a new clearance shall be made in accordance with paragraph 24b. If a contractor reemploys an individual who previously held a contractor-granted clearance at that facility, all of the actions required by paragraph 24b shall be accomplished, except for verification of U.S. citizenship. *

(3) An LAA is not transferrable except in the case of an MFO. *

e. Clearance Transfers in an MFO. Clearance transfer action under this paragraph shall be initiated after a determination to reassign has been made, but prior to the actual transfer.

(1) When a cleared employee is transferred from one cleared facility to another with the same or higher level FCL, the contractor shall:

(a) forward the original LOC 6/ or the DD Form 48-2, as appropriate, to the gaining facility; and

(b) promptly submit a DISCO Form 562 to DISCO as notification of the transfer if the clearance is government-granted and forward a copy of the DISCO Form 562 to the gaining facility.

(2) When a cleared employee is transferred to an uncleared facility or to a facility with a lower level FCL than the employee's clearance, and the employee will continue to require access at the higher level at another cleared facility or at a U.S. Government installation, the contractor shall:

(a) forward the original LOC 6/ or the DD Form 48-2, as appropriate, to the HOF or the appropriate PMF rather than to the gaining facility, and

(b) submit a DISCO Form 562 to DISCO identifying the HOF or PMF holding the employee's PCL if the clearance is government-granted.

(3) When a cleared employee is transferred to a cleared facility with a lower level FCL than the employee's clearance and the contractor desires to retain the LOC only at the lower level, the contractor shall:

(a) amend the employee's LOC to reflect the lower level of clearance; and

(b) add a statement regarding the change in level of clearance to the "Remarks" block of the DISCO Form 562 and promptly submit the form to DISCO.

f. Concurrent Clearances. *

(1) When a contractor hires an individual or engages a consultant *
on a temporary or part-time basis, who is also employed by or acting as a *
consultant to another contractor, and who has a current LOC, an additional *
LOC shall be requested, if the individual requires access to classified *
information. Application for this LOC will be made by the submission to *
DISCO of DD Form 48-3 (with the "Concurrent" clearance block marked on *
part I). *

(2) Any action by the U.S. Government to suspend or revoke a clearance will be equally applicable to all concurrent clearances issued. Concurrent notices of such action will be provided to each employer by the U.S. Government.

6/ If the LOC contains more than one name, a certified true copy identifying the employee being transferred shall be forwarded. All other names listed shall be lined through.

g. Reserved.

h. Letters of Consent (LOC) (DISCO Form 560). The LOC is issued by DISCO to notify the contractor that one of its employees is cleared for access to classified information at the classification level indicated thereon. The LOC's must be maintained by the contractor to facilitate review by the CSO during on-site inspections.

(1) Issuance of LOC's (General).

(a) LOC's are issued to the facility where the individual is principally employed.

(b) LOC's may not be issued for a higher level of access than the FCL of the facility where the employee is principally employed.

(c) LOC's may not be reproduced except for the necessary records of the contractor or unless requested by competent U.S. Government authority.

(d) LOC's may not be released, nor copies provided, to the employee.

(e) Whenever there is a change in the legal name of an employee for whom an LOC has been issued, the contractor shall submit one copy of DISCO Form 562 to DISCO. DISCO will issue a new LOC.

(f) The LOC shall be returned to DISCO upon death of an employee, or whenever return is requested by the U.S. Government.

(2) Issuance of LOC's in an MFO. The home office facility (HOF) may elect to establish a PMF at other cleared facilities within the MFO to be responsible for personnel security administration in a specific geographic or functional area as prescribed by paragraph 73. In such cases, the LOC may be issued to either the home office or the PMF. However, it may not be at a higher level that the FCL of the facility to which issued.

(a) When a cleared employee's duties at another facility or a U.S. Government installation require access to classified information at a higher level than the clearance of the facility where the employee is employed or physically located, or if the employee is employed at an uncleared facility, the LOC may be issued to the HOF or to an appropriate PMF.

(b) When an employee is cleared in connection with the home office FCL, and the employee's principal place of work is at another facility of the MFO, the LOC is issued to both the home office and the facility where the employee is employed or physically located or to an appropriate PMF. The contractor shall submit a DISCO Form 562 to explain and justify the reason for requesting an additional LOC.

(c) On the DD Forms 48, 49, 48-3, or DISCO Form 562 submitted pursuant to (a) or (b) above, the name and address of the facility at which the employee is employed or physically located shall be shown in the "Name and Address of Employer" block of the form. The name and address of the facility to which the LOC is to be mailed shall be placed in the "REMARKS" block of the form preceded by the words "MAIL TO" in bold letters.

27. Conversion of Clearances of Present and Former Civilian and Military Personnel of the DoD and Other Government Agencies to Industrial Clearances. PCL's granted by UAs and other government agencies to personnel who are U.S. citizens may be converted to industrial PCL's when: (i) a determination can be made, based on a review of the prior investigation, that the investigation meets the standards prescribed by the DoD for such clearances, (ii) an inquiry to the employee's previous employer or employers discloses no reason for expanding or updating the investigation, and (iii) not more than 24 months has elapsed since the date of termination of the PCL. The complete set of forms as required by paragraph 26b (new clearances) shall be completed when (i) the clearance requirement is for a higher level of access than is reflected in the clearance records, (ii) there has been a greater lapse of time than 24 months since termination of the PCL, and (iii) requested by DISCO. (The request will state that the forms are needed to satisfy an official requirement.)

a. U.S. Government Personnel. Contractors shall request clearance by submitting a completed DD Form 48-3 to DISCO along with a copy of the "Notification of Personnel Action," (Standard Form 50), which terminated employment with the U.S. Government. If the individual is still presently employed by the UA, submission of SF 50 is not required.

b. Military Personnel. Application for a PCL for former military personnel shall be requested by submitting a completed DD Form 48-3 to DISCO along with a copy of the DD Form 214, "Certificate of Release or Discharge from Active Duty." In the case of military personnel who are still on active duty, only a copy of the DD Form 48-3 need be submitted to DISCO; however, the individual's service number shall be reflected in the "REMARKS" section.

c. National Guard and Reserve Military Personnel in the Ready Reserve Program. Clearances on personnel actively participating in the Ready Reserve Program or who have transferred to the standby or retired Reserve within the past 24 months shall be requested by submitting a completed DD Form 48-3 to DISCO. The individual's service number, the identity and exact address of the unit to which assigned, and the date such participation commenced, shall be placed in the "REMARKS" section of the DD Form 48-3. For those individuals who have transferred to the standby or retired Reserve, a copy of the order affecting such transfer shall be attached to the DD Form 48-3.

d. DOE (Previously ERDA) and NRC Clearances. The "Q" and "L" clearances granted by DOE and NRC are acceptable for conversion to a DoD industrial PCL. The "Q" clearance is considered an authoritative basis for a DoD clearance at the TOP SECRET level, and the "L" clearance is considered an authoritative basis for a DoD clearance at the SECRET level. A contractor may request a DoD industrial PCL for an employee who currently has a "Q" or "L" clearance or previously held such a PCL when there has been a lapse of not more than 24 months since termination of the PCL.

Application for conversion of the "Q" or "L" clearance shall be made by submitting the DD Form 48-3 to DISCO. The "Job Title" block in part I of the DD Form 48-3 will be annotated: "DOE (or NRC) 'Q' (or 'L') Conversion Requested." The "Q" or "L" number, if known, will be indicated. Following verification of the clearance information with DOE or NRC, DISCO will issue an LOC to the contractor.

28. Contractor's Clearance Record. The contractor shall maintain a current record at each facility (to include uncleared locations) of all employees and consultants located at the facility or uncleared location who have been authorized access to classified information. The record shall indicate the level of access authorized and the date of the applicable LOC. The record shall also reflect the issuing authority, that is, a specific military department, DISCO, or the contractor. Moreover, the records maintained by a HOF and/or PMF for employees located at subordinate facilities (cleared and uncleared locations) shall include the name and address at which the employee is assigned. In addition, contractors shall maintain the DIS FL 381-R, the DD Form 441 or DD Form 441-1, for the duration of their facility security clearance. In the event the Security Agreement is terminated for any reason by either party, the DIS FL 381-R and the contractor's copy of the DD Form 441, or the DD Form 441-1, shall be returned to the CSO.

29. Administrative Termination of Personnel Security Clearances.

a. The contractor, under the conditions stated below, must administratively terminate U.S. Government granted PCL's which are no longer required. If a cleared employee no longer has or requires access to classified information, and no requirement for such access is anticipated in the foreseeable future (approximately 120 days), administrative termination of a U.S. Government issued clearance shall be accomplished by submission of a properly completed DISCO Form 562 to DISCO. Contractor-granted CONFIDENTIAL clearances and LAAs must also be administratively terminated by the contractor in accordance with the criteria of this paragraph.

b. If the contractor determines that an individual previously cleared in connection with the FCL no longer requires clearance and can be excluded from access, a recommendation for administrative termination of the clearance must be submitted to the CSO by submission of a properly completed DISCO Form 562 and two copies of the organization's minutes attesting that the exclusion action required by paragraph 22e has been completed.

c. When administratively terminating a PCL, the contractor shall advise the employee as follows:

(1) the PCL is being processed for administrative termination since there is no current or foreseeable future requirement for access to classified information;

(2) the proposed action in no way reflects adversely on the employee's PCL eligibility;

(3) the employee may be processed for a new PCL, with a minimum of delay, when the occasion and need arises for the employee to require access to classified information; and

(4) the employee's signature on the Security Debriefing
Acknowledgement portion of the SF 312 will attest to the fact that he or *
she understands and acknowledges this action.

d. A completed DISCO Form 562 will be forwarded to DISCO when admin- *
istratively terminating a U.S. Government issued PCL or an LAA. (In the *
case of an OODEP, the DISCO Form 562 shall be forwarded to the CSO.) In the *
case of the administrative termination of a contractor-granted CONFIDENTIAL *
clearance, the DD Form 48-2 will be annotated "Administratively terminated *
(date)" and the annotation will be signed by the contractor. (Upon termina- *
tion of employment, the DD Form 48-2 will be similarly annotated "Employ- *
ment and PCL terminated (date)"). *

e. The completed SF 312 will be retained by the contractor, in accordance with paragraph 5g. If it becomes necessary to revalidate the clearance, a new SF 312 shall be executed prior to the employee having access to classified information.

f. In those rare and exceptional cases where DUSD(P), or higher authority, determines that PCL's were granted in error or are not required, he or she may opt to administratively terminate the PCL or clearance action in process without prejudice to the individuals concerned or jeopardy to their employer's operations.

g. In the event a need arises for an employee to have access to
classified information subsequent to the administrative termination of
the employee's PCL, and such need occurs within 5 years from the date of
the notice to the U.S. Government that the previous clearance was admin-
istratively terminated, the previous clearance may be reinstated provided:
(i) the employee has been continuously employed by the same contractor
during the 5-year period, (ii) no adverse information concerning the
employee is known to the contractor, and (iii) the reinstatement is fully
justified. The reinstatement shall be accomplished by submission of a
DD Form 48-3 to DISCO with certification, in "Remarks," that no break in *
employment has occurred since the employee's previous clearance was
administratively terminated, nor is any adverse information known to the
contractor about his/her employee. If the clearance is not eligible for
reinstatement in accordance with this procedure, an application for new
clearance shall be submitted in accordance with paragraph 26b.

h. If the administratively terminated clearance had been a contractor-granted CONFIDENTIAL clearance, and there is a subsequent need for the individual to have access to CONFIDENTIAL information, the actions required by paragraph 24b shall be accomplished as a new clearance action.

i. Administratively-terminated LAAs for immigrant aliens may be *
reinstated as provided for in paragraph 31.1e. *

30. Administrative Downgrading of Personnel Security Clearances.

a. Contractors shall take action to administratively downgrade a TOP SECRET or SECRET PCL when an employee no longer has or requires access to classified information at the level of the existing clearance, but access to a lower level of classified information is required. The PCL shall be downgraded without prejudice by submission of a DISCO Form 562 to DISCO. The "Remarks" block shall reflect the request to downgrade the TOP SECRET or SECRET clearance without prejudice to the appropriate level. On notification of completed action by DISCO, the contractor shall annotate the previously issued LOC to reflect the new level of access and the date such action was taken by DISCO. The LOC retains the original date of issuance.

b. PCL's downgraded in accordance with paragraph a above, can be reinstated by the contractor when a requirement for higher level access
exists provided that: (i) there has not been a lapse of more than 5 years *
from the date of the downgrading, (ii) the individual has been contin- *
uously employed by the same contractor, and (iii) a justified need exists *
for the upgrade action. Upon reinstatement of a TOP SECRET or SECRET PCL, *
the contractor shall notify DISCO of the upgrading action by submission of *
a completed DISCO Form 562. The "Remarks" section of the DISCO Form 562 *
shall include the date of reinstatement, the level of clearance and a request for a new LOC. On receipt of the LOC from DISCO reflecting the upgrading action, the previously issued LOC will be destroyed by the contractor. The LOC will bear a new date of clearance because of the upgrading action. When there has been a lapse of more than 5 years from the date the clearance was downgraded to a lower level, application for a TOP SECRET or SECRET PCL shall be made by submission of the DD Form 49 or DD Form 48, as appropriate, to DISCO.

31. Access to Classified Information by Non-U.S.Citizens. Only U.S. citizens are eligible for a security clearance and every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, immigrant aliens or foreign nationals may be granted a "Limited Access Authorization" (LAA) at the SECRET or CONFIDENTIAL level, if qualified, as described below.

31.1 Immigrant Aliens.

a. An immigrant alien may be eligible for an LAA when all of the following conditions are met:

(1) the minimum age requirement (at least 21 years) has been met; *

(2) access is limited to a specific government contract;

(3) the individual possesses a rare or unusual expertise;

(4) a qualified U.S. citizen cannot be hired in sufficient time to meet a contractual requirement;

(5) the individual resides permanently in the U.S. and presents for verification an "Alien Registration Receipt Card" (Form No. I-151 or I-551 7/); and

(6) the individual certifies in writing the intent to become a U.S. citizen as soon as eligible.

b. Prior to requesting an LAA, the proposal shall be endorsed, in writing, by the UA authority with jurisdiction over the contract for which access is proposed.

c. After endorsement has been obtained from the contracting officer, the request for an LAA shall be submitted as provided for in paragraph 26b. The endorsement must include a statement or evidence that a favorable foreign disclosure decision has been rendered. If determined eligible by the Government, an LOC will be issued by DISCO to reflect the LAA and the level of access authorized. The LOC will include the words "Limited Access Authorization - Immigrant Alien."

d. Record Keeping. In each case where an LAA has been granted to an immigrant alien, the contractor shall maintain, for as long as the LAA is in effect, a record of the following information:

(1) the identity (including current citizenship) of the individual to whom the LAA is granted, to include, name, and date and place of birth;

(2) date of LAA, the issuing authority, and a copy of the correspondence from the UA authority who endorsed the LAA;

(3) the nature of the specific program material(s) to which access is authorized and expressly limited (delineated as precisely as possible);

(4) the classification level to which access is authorized

(5) the compelling reasons for granting access (a copy of the justification request forwarded to the contracting officer may be sufficient);

7/ This card is issued only to aliens who have been lawfully admitted to the U.S. under an immigration visa for permanent residence. Pending issuance of the new Form I-551, the Immigration and Naturalization Service has authorized the following notation to be stamped on officially issued documentation as evidence of immigrant alien registration:

PROCESSED FOR I-551. TEMPORARY EVIDENCE OF LAWFUL ADMISSION FOR PERMANENT RESIDENCE VALID UNTIL EMPLOYMENT AUTHORIZED.

(6) evidence of a favorable decision from designated U.S. Government foreign disclosure authority concerning the releasability of the information approved for disclosure; and

(7) the period of time for which access is authorized or anticipated.

e. Upon completion of the last contract for which access was authorized, the contractor shall request the administrative termination of the LAA by forwarding to DISCO a properly completed DISCO form 562, as outlined in paragraph 29d. In the event that revalidation is necessary for access under a new contract, the contractor shall submit a DD Form 48-3 to DISCO along with the UA endorsement as specified above. A new LOC will be issued provided the immigrant alien (i) is not yet eligible for U.S. citizenship, (ii) has been continuously employed by the same contractor since termination of the LAA, and (iii) no adverse information is known to the contractor. * * * * * * * * * *

31.2 Foreign Nationals.

a. Foreign nationals may be eligible for an LAA only when:

(1) access to classified information is proposed in connection with the granting of an FCL to a firm in the U.S. under foreign ownership, control, or influence (FOCI) by a country source of which the individual is a citizen; or

(2) access to classified information is required at a contractor facility for performance on a contract or subcontract involving the government of the individual's country of citizenship; and

(3) there is a bilateral security agreement containing provisions for the exchange of security assurances between the U.S. Government and the government of which the individual is a citizen.

b. Information concerning documentation to be submitted for an LAA application shall be obtained from DISCO. Upon receipt of the appropriate security assurance from the foreign government, an LOC will be issued by DISCO to record the LAA status and reflect the level of access authorized. The LOC will include the words "Limited Access Authorization - Foreign National." If the LAA is granted in connection with a freight forwarder clearance, the LOC will also be annotated "FREIGHT FORWARDER CLEARANCE." Foreign national access approvals granted pursuant to previous DoD policy will be evaluated for continuing eligibility. * * *

31.3 Access Limitations for Immigrant Aliens, Foreign Nationals, and Firms Granted a Reciprocal Facility Security Clearance. Reciprocal FCL's and all LAA's granted under the provisions of this manual are not valid for access to:

a. TOP SECRET information;

b. Information that has not been determined releasable by designated U.S. Government disclosure authorities to the country of which the individual is a citizen or, in the case of a reciprocal FCL, to the country from which the FOCI is derived;

c. RESTRICTED DATA, as defined in the U.S. Atomic Energy Act of 1954, as amended;

d. FORMERLY RESTRICTED DATA removed from the RESTRICTED DATA category pursuant to Section 142(d), Atomic Energy Act of 1954, as amended;

e. COMSEC information;

f. NATO information, except as provided for in paragraph 86.

g. ACDA classified information;

h. information for which foreign dissemination has been prohibited in whole or in part;

i. information for which a special access authorization is required; and

j. information provided to the U.S. Government in confidence by a third party government and classified information furnished by a third party government.

Section IV. CONTROL OF AREAS

32. Purpose. Normally, the contractor shall protect classified material in the manner prescribed in paragraphs 14, 15, and 16. If, however, because of the nature, size, or unique characteristics of the classified materials, unauthorized personnel cannot be effectively denied access to such material by the safeguards set forth in the above paragraphs, the material shall be safeguarded by controlling the area in which it is located 1/. Controlled areas shall consist of closed and restricted areas as defined in paragraphs 3m and 3bx, respectively.

33. General.

a. A controlled area shall not be established for the sole purpose of storing classified documents (see paragraph 14a(3)(f) for guidance on use of "other vaults and strongrooms" for the storage of classified documents).

b. Area Approval. The CSO and the contractor shall agree on the need to establish, and the extent of, the controlled area prior to the award of the contract, when possible, or at such subsequent times as the need for such areas becomes apparent during the performance on the contract.

c. Reports. The CSO shall be advised, in accordance with paragraph 6a(5), of the establishment of any new controlled areas or of any change in the location or extent of any existing controlled areas. Controlled areas which have been temporarily deactivated, in accordance with e below, and subsequently reactivated within 180 days need not be reported.

d. A controlled area shall be disestablished when the original or existing need for the creation of the area no longer exists (for example, all classified material is removed from the area for delivery to the customer), and there is no anticipated need to reactivate the area within 180 days. Area designations shall be promptly removed when controlled areas have been disestablished. If a disestablished controlled area is subsequently reestablished, it must be approved as a new area in accordance with b and c above.

e. Controlled areas shall be considered temporarily deactivated when a controlled area environment is no longer required (see paragraph 32), and there exists a known or anticipated need to reactivate such areas within 180 days. The area controls specified in paragraphs 34a and b are optional, except that posted area designations shall be promptly removed or covered. Temporarily deactivated controlled areas shall be considered disestablished if the need to reactivate fails to materialize within the above 180-day time frame.

1/ The entry into a controlled area, per se, will not constitute access to classified information if the security measures that are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a PCL.

34. Area Controls.

a. Closed Areas.

(1) General. Closed areas shall be separated from adjacent areas by a physical barrier capable of preventing unauthorized entry and, when visual access to classified materials is a factor, observation by unauthorized persons. The physical barrier shall be substantially constructed of materials that provide protection against surreptitious entry or removal of classified material, and offer visual evidence of attempted surreptitious or forced entry (see appendix V for construction requirements). Closed areas shall be physically configured, in conjunction with internal personnel controls and procedures, in a manner that reasonably forecloses the possibility that unauthorized personnel can transgress the area undetected. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority, regardless of the nature of perimeter controls in use.

(2) During Working Hours.

(a) Open or unlocked entrance -- if the material within the area is classified no higher than CONFIDENTIAL, admittance shall be controlled by a properly cleared contractor-authorized employee or guard stationed so as to supervise the entrance to the area. If the material is classified TOP SECRET or SECRET, admittance shall be under the direct and continuous supervision of a properly cleared guard posted at the entrance.

(b) Locked entrance -- if the material within the area is classified no higher than SECRET, admittance shall be under the direct and continuous supervision of a properly cleared contractor-authorized employee or guard, except as may be provided for by complying with paragraph 36. The employee or guard designated to control the entrance shall be required to unlock and open the entrance, remain at the entrance while it remains open, supervise the passage of material or authorized personnel through the entrance, and to lock the entrance immediately thereafter. If the material is classified TOP SECRET, admittance shall be under the direct and continuous supervision of a properly cleared guard posted at the entrance, except as may be provided for by complying with paragraph 36.

(3) During Nonworking Hours.

(a) Admittance shall be controlled by locked entrances and exits, secured with either a built-in three-position dial-type changeable combination lock or a three-position dial-type changeable combination padlock as described in paragraph 14a(3)(d). However, doors secured from the inside with a panic bolt (that is, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSO, will not require additional locking devices.

(b) If TOP SECRET or SECRET information is stored in the area, supplemental controls are required, as follows:

1 the area shall be equipped with an IDS, in accordance with the requirements of paragraph 35; or *

2 the area shall be patrolled by guards or other properly cleared and authorized personnel supervised by a system which provides a written record of the coverage of key points of the area. The patrol shall be once hourly for TOP SECRET areas and once every two hours for SECRET areas. The guard shall view both the inside and outside of the area to determine the presence of unauthorized persons. Guards are not required to enter the closed area, if substantially all of the interior space can be viewed from outside the area through windows, peepholes, or expanded metal/wire-mesh walls. (Drapes, curtains, or similar window coverings may be utilized during working hours and tarpaulins over hardware during nonworking hours to protect classified external configuration from visual access.) If the contractor elects to have the guard enter the closed area, an approved key-operated padlock 2/ with high-security cylinder may be used to secure the area. If the contractor does not want to have the guard enter the closed area and if windows, peepholes, or expanded metal/wire-mesh walls cannot be used, because exterior configuration of hardware is classified and the use of tarpaulins to prevent visual access is not practical, the contractor may elect to utilize the following alternative procedure:

> The area will be thoroughly checked at the end of the working hour period by the last person leaving to ensure area integrity and that no individual remains within. A written record, to include the signature of the person securing the area and the time secured, will be posted on the interior side at the door. Additionally, a log will be posted at the exterior of each door and the guard will

---

2/ Approved key-operated padlocks shall meet the requirements of: Military Specification P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, and Military Specification P-43951 (regular shackle), National Stock Number 5340-00-799-8016. The keys shall be safeguarded as classified material of a classification equal to the highest level of the classified material being protected. On initial receipt, or when not in use, high security key locks shall be stored consistent with the level of the facility's authorized safeguarding capability. Use of key-operated padlocks are subject to the following requirements: (i) a key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified material; (ii) a key and lock control register shall be maintained to identify keys for each lock and their current location and custody; (iii) keys and locks shall be audited each month; (iv) keys shall be inventoried with each change of custody; (v) keys shall not be removed from the premises; (vi) keys and spare locks shall be protected in a secure container; (vii) locks shall be changed or rotated at least annually, and shall be replaced after loss or compromise of their operable keys; and (viii) making master keys is prohibited. A "secure container" as used herein is any cabinet or vault specified in paragraph 14a(3), including supplemental controls when required. However, at no time shall a key(s) be afforded less protection than that accorded the highest level of the classified material protected by its corresponding lock(s).

be required to sign and indicate the time checked, certifying that the door was checked and found to be locked during the course of each patrol.

The SPP shall specify which of the above options has been elected by the contractor and shall describe the procedures for implementing this requirement.

(c) No patrol or alarm systems are required for CONFIDENTIAL material stored in closed areas.

(4) Areas shall be designated and marked "CLOSED AREA."

(5) Employees assigned to the area shall challenge the presence of any unknown persons. The need-to-know principle shall be adhered to at all times within the closed area.

b. Restricted Areas.

(1) During working hours, the same controls as prescribed for closed areas during working hours shall be applied.

(2) During nonworking hours, the same controls as prescribed by paragraph 14 shall be applied.

(3) Areas shall be designated and marked "RESTRICTED AREA."

c. Area Approval. The CSO and the contractor shall agree on the extent of the controlled area prior to the award of the contract, when possible, or at such subsequent times as the need for such areas becomes apparent during the performance on the contract. When the costs of construction and/or maintenance of the controlled areas are to be charged against a UA contract, the CSO shall obtain and furnish to the contractor written authorization from the contracting officer concerned for the expenditure of necessary funds. This authorization shall only be required when the contractor is performing on cost-reimbursement contracts as opposed to fixed-price contracts in which such security costs would be included in the initial contract price.

d. Reports. The CSO shall be advised, in accordance with paragraph 6a(5), of the creation of any new controlled areas or of any change in the location of any existing controlled areas.

35. Supplemental or Supplanting Intrusion Detection Systems (IDS). *

a. IDS may be divided into those that supplant (replace) guards required under paragraph 34a(3), and those that supplement (extend the capability of) guards. * * *

(1) When used to supplant guards, the IDS shall be connected to and monitored by a central control station. * *

(a) The central control station may be located at the contractor's facility, in which case it is known as a proprietary central supervising station, or at a commercial central station listed with Underwriters Laboratories Incorporated (U.L.).

(b) In exceptional cases, an IDS connected by direct wire to a local police department may be considered. Specific guidance for this type installation is contained in Appendix XI to this manual.

(c) For either a proprietary central supervising station or commercial central station, trained alarm monitors, cleared to the SECRET level, shall be in attendance at the station at all times when the IDS is in operation.

(d) For a proprietary central supervising station, trained guards, cleared to the SECRET level and sufficient in number to dispatch immediately to investigate each alarm, shall be available at all times when the IDS is in operation. (If a commercial central station dispatches guards, they shall be cleared only if they have the ability and responsibility to access the area or container(s) housing classified material, i.e., if keys to the facility have been provided to responding guards and the guards have specific orders to enter the building for the purpose of checking the container or area which contains classified material.)

(e) A signal shall be maintained at the central control station to show whether or not the system is in working order and to indicate tampering with any element of the system. Necessary repairs shall be effected within 24 hours. (In those cases where repairs on an IDS protecting classified material cannot be completed within 24 hours, the contractor of the alarmed facility shall be responsible for stationing an employee, cleared SECRET, at the alarmed site until repairs are completed.)

(f) Response time to an activated alarm (that is, the time required for guards to reach the alarmed area) shall not exceed 15 minutes from the time the alarm was first registered except as provided for in appendix XI to this manual.

(g) Specific requirements regarding equipment, installation, operation, and approval of IDS used to supplant guards are contained in appendix XI to this manual.

(h) Records shall be maintained indicating time of receipt of alarm, name of guards responding, time dispatched to facility/area, time guards arrived, nature of alarm, and what follow-up actions were accomplished. Such records shall be kept for a minimum of 1 year.

(i) Guards dispatched by a commercial central station to a cleared facility's alarm shall remain on the premises until a designated, cleared representative of the facility arrives, or for a period of not less than one hour, whichever comes first. If a cleared representative of the facility does not arrive within one hour following the arrival of the guard, the commercial central station must provide the CSO with a report of the incident that includes the name of the subscriber facility, the date and time of the alarm and the name of the subscriber's representative who was contacted to respond. This report should be submitted within 24 hours of the next working day.

(j) When IDS are used, they shall be activated immediately at the close of business at the area or container that is safeguarded by the IDS. This may require that the last person who departs the controlled area or container notify the control station to set the alarm. A written record of the setting of the alarm shall be maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate shall be reported to the FSO. Such records shall be maintained for at least 30 days.

(2) IDS utilized to supplement guards. When used to extend the capabilities of guards as provided for in paragraph 34a(3), the IDS need not be monitored by a central control station. If not monitored by a central control station, the IDS shall provide an audible or visual alarm signal capable of alerting guards on patrol in the area and directing them to the location of the alarm. In any event, the time required to respond to an activated alarm shall not exceed 15 minutes.

b. IDS Material and Installation Standards

(1) All IDS material and equipment shall equal or exceed, and shall be installed in accordance with, the standards cited in paragraphs C. and D. of appendix XI to this manual.

(2) When individual alarm sensors are installed on classified storage containers, in accordance with paragraph 14a(2)(c) or 14a(4)(c), the installation shall provide "complete" protection as provided for in the U.L. listing system. In addition, when supplanting guards, the requirements for connection to a central control station or a direct-connect alarm system shall apply (see appendix XI to this manual).

c. Approval by the CSO is required before the installation of either a supplanting or supplemental IDS to meet the requirements of this manual (see paragraph 34c regarding cost considerations).

d. Intrusion detection systems installed after the effective date of this manual are required to meet the criteria of this paragraph and appendix XI to this manual. IDS currently in use which do not meet these criteria (such as (i) those certified to meet Grade A service, (ii) those installed by a non-U.L. listed alarm company, or (iii) those installed at cleared facilities by in-house personnel) may continue in use until disestablishment of the area or condition for which the IDS was initially installed. If the area is re-established and an IDS is to be employed in lieu of guards, the IDS must conform to the standards of this paragraph.

36. Supplanting Access Control System Devices.

a. Automated Access Control Systems. Automated access control systems which meet the criteria stated below are authorized to supplant contractor-authorized employees or guards required by paragraph 34a(2)(b) for controlling admittance to controlled areas during working hours 3/.

(1) The automated access control system must be capable of identifying the individual entering the area and authenticating that person's authority to enter the area.

(2) Identification of individuals entering the area can be obtained by an identification (ID) badge or card, or by personal identity verification.

(a) ID badge or card. The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(b) Personal identity verification. Personal identity verification identifies the individual requesting access by some unique personal characteristic, such as:

1 fingerprint,
2 hand geometry,
3 handwriting,
4 retina, or
5 voice recognition.

(3) In conjunction with (2)(a) or (b) above, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device. The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

(4) Authentication of the individual's authorization to enter the area must be accomplished within the system by comparing the inputs from the ID badge/card or the personal identity verification device and the keypad with an electronic data base of individuals authorized into the area.

3/ Manufacturers of automated access control equipment or devices must assure in writing that their system will meet the following standards before CSO's may favorably consider such systems for protection of classified information:

Chances of an unauthorized individual gaining access through normal operation of the equipment are no more than one in ten thousand.

Chances of an authorized individual being rejected for access through normal operation of the equipment are no more than one in one thousand.

A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's PCL is suspended, revoked, or downgraded to a level lower than required.

(5) Physical security protection must be established and continuously maintained for all devices/equipment that constitute the system. The level of protection may vary depending upon the type of devices/equipment being protected with the basic intent of utilizing the security controls already in effect within the contractor's facility.

(a) Locations where access transactions are, or can be displayed, and where authorization data, card encoded data and personal identification or verification data is input, stored, displayed, or recorded must be protected. This protection may be accomplished by continuous surveillance by authorized personnel, structural safeguards as described by Appendix V, or a level of collective controls developed by the contractor keyed to the prevention or detection of unauthorized access or system modification.

(b) Control panels, card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall have tamper resistant enclosures, be securely fastened to a wall or other structure, be protected by a tamper alarm or secured with a three-position dial-type changeable combination padlock. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism. Where areas containing TOP SECRET information are involved, tamper alarm protection is mandatory.

(c) Keypad devices shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the selection of push buttons.

(d) Systems that utilize transmission lines to carry access authorization, personal identification, or verification data between devices/equipment located outside the controlled area shall receive circuit protection equal to or greater than that specified as Grade A by Underwriters' Laboratories, Inc.

(6) Access to records and information concerning encoded ID data and PINs shall be restricted to individuals cleared at the same level as the highest classified information contained within the specific area or areas in which ID data or PINs are utilized. Access to identification or authorization data, operating system software or any identifying data associated with the access control system shall be limited to the fewest number personnel as possible. Such data or software shall be kept secured when unattended.

(7) Records reflecting active assignments of ID badges/cards, PINs, levels of access, PCL's, and similar system related records shall be maintained indefinitely. Records concerning personnel removed from the system shall be retained for one year. Records of entries to controlled

areas containing TOP SECRET material shall be retained for at least 6 months or until investigations of system violations and incidents have been successfully resolved and recorded.

(8) Personnel entering or leaving an area shall be required to immediately secure the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's PCL and need-to-know.

(9) During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized employee or guard stationed to supervise the entrance to the area.

b. Electric, Mechanical, or Electromechanical Devices.

Provided that the material within the controlled area is classified no higher than SECRET, electronic, mechanical, or electromechanical devices which meet the criteria stated below may be used to supplant contractor-authorized employees or guards to control admittance to controlled areas during working hours. Devices may be used that operate by either a push-button combination which activates the locking device or by a control card used in conjunction with a push-button combination, thereby excluding any system that operates solely by the use of a control card.

(1) The electronic control panel containing the mechanical mechanism by which the combination is set may be located inside or outside the controlled area. When located outside the controlled area, the control panel shall be securely fastened or attached to the perimeter barrier of the area and secured by an approved three-position dial-type changeable combination padlock. If the control panel is located within the controlled area, it shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

(2) The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the selection of the correct combination of the push buttons.

(3) The selection and setting of the combination shall be accomplished by an employee of the contractor who is authorized to enter the area in his or her duties or by the FSO or his or her designated representative who is authorized to enter the area. The combination shall be changed at least once every three months.

(4) The combination shall be classified in accordance with the classification of the highest classified material within the controlled area (see paragraph 8 for control of cards).

(5) Electrical gear, wiring included, or mechanical links (cables, rods and so on) shall be accessible only from inside the area, or shall be secured within a protecting covering to preclude surreptitious manipulation of components.

(6) Personnel entering or leaving the area shall be required to immediately lock the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's PCL and need-to-know.

(7) During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized employee or guard stationed to supervise the entrance to the area.

c. Approval by the CSO is required before effecting the installation of a supplanting access control device to meet a requirement of this manual (see paragraph 34c regarding cost considerations).

Section V. VISITOR CONTROL PROCEDURES

Part 1. VISITS TO USER AGENCY CONTRACTORS

37. General.

a. The provisions of this section, except paragraphs 45 and 48, apply only to persons who will have access to classified information. Access to information classified higher than the level in the visit authorization will not be granted, regardless of the level of the visitor's PCL. The contractor or activity being visited shall take such security measures as may be required to preclude visitors from having unauthorized access to classified information. Nothing in this section will limit the requirements of paragraph 5c.

b. The number of visitors requiring access to classified information shall be held to a minimum and the following requirements must be established:

(1) that the visit is necessary, and

(2) that the purpose of the visit cannot be achieved without access to classified information by the visitor.

c. In the event the visit is disapproved, the requester shall be promptly notified by the contractor or activity which made the decision.

d. Requests for visits shall be furnished in writing (mail, facsimile, or teletype) to the contractor or UA activity being visited in advance of the proposed visit. In exceptional cases, the telephone may be used, provided the visit request is confirmed in writing. Under no circumstances, however, may visit requests be handcarried to the place being visited. All Category 1 and 2 requests shall contain the following information: * *

(1) name and address of the contractor or UA activity to be visited;

(2) name and title of person(s) to be visited, if known;

(3) name of the proposed visitor, his or her date and place of birth, and citizenship (if immigrant alien, so indicate);

(4) job title or position of the proposed visitor;

(5) requesting contractor's or UA activity's certification of the level of clearance of the proposed visitor (see paragraph 38). If the visitor possesses an interim PCL, a contractor-granted CONFIDENTIAL PCL, or an LAA, so indicate. See paragraph e below for special access requirements;

(6) purpose and justification for the visit in sufficient detail to allow for a determination for the necessity of the visit -- including the

contract, project, or program number or name will assist the recipient in making this determination 1/;

(7) date or period during which the request is to be valid;

(8) name, address and Commercial and Government Entity (CAGE) identification number of the contractor or the name and address of the UA activity; and *

(9) the requesting contractor's certification of his or her FCL (not required for representatives of the U.S. Government, see paragraph 38); if the contractor has a reciprocal FCL, so indicate.

e. When visits involve access to classified information requiring a special access authorization (for example, CRYPTO, NATO, or special or limited access programs), the request will, in addition to the other required information:

(1) specify the program or project,

(2) specify the level of information to be released,

(3) certify that the visitor has been authorized access to such information, and

(4) identify the office or UA activity granting such authorization.

f. When appropriate, the visit request shall ask for approval for subsequent visits within a 12-month period. The contractor or UA activity initiating the visit request shall immediately notify the contractor or activity being visited of any change in the visitor's status, such as, the termination of employment, suspension of employment, leave of absence, and the suspension, revocation, administrative termination or the downgrading of clearance, which will require the visit authorization to be canceled or amended, as appropriate, prior to its normal termination date. In the event the initiating contractor's FCL, as indicated in paragraph d(9) above, changes to a reciprocal clearance, the initiating contractor shall immediately notify contractors or UA's honoring current visit requests, so as to preclude the visitor's access to certain types of classified information as set forth in paragraph 31c. A downgrading or termination of the FCL also requires an immediate notification to contractors and UA's honoring current visit requests.

g. Machine-run or other rosters of employees, limited to those personnel who are authorized access to particular levels of classified information and who occupy positions which require classified visits, may be used for establishing visit request and approval authorizations as required by this section, provided the machine-run (or other roster) or a covering letter furnishes the

---

1/ To avoid delay in processing or rejection of visit requests, contractors should exercise care in using nicknames, abbreviations, and acronyms which may be unfamiliar to the recipient. Where repeated use of short terms is desirable for brevity, an explanation should be provided.

essential information required by paragraphs d, e, and f above, and adequate procedures are in effect to notify the visited facility of changes in employees' status, which will affect his or her visit authorization. Use of such procedures must be acceptable to the facility being visited and such records and controls shall be maintained in a current status at all times.

h. Industrial Security Representatives of the DoD and other UA's, when acting in their official capacities, and representatives of the following U.S. Government agencies may visit contractor facilities without having furnished advance notification of their intent to visit:

(1) Defense Investigative Service

(2) Inspector General, Defense Criminal Investigative Service (DoD)

(3) U.S. Army Intelligence Command (Army)

(4) Naval Investigative Service Command (NISC)

(5) U.S. Air Force, Office of Special Investigations (Air Force)

(6) Secret Service (Treasury Department)

(7) Federal Bureau of Investigation

(8) National Security Agency, Central Office of Record *

The contractor shall grant access to classified information to the minimum required upon presentation of proper credentials by the representative. In case of doubt as to identity or level of access authorized, such credentials and level of clearance shall be verified by contact with the agency or activity concerned.

38. Identification and Control of Visitors.

a. Contractors being visited by representatives of another contractor are responsible for determining that the requesting contractor has been granted an appropriate FCL. This determination is based either on an existing contractual relationship involving classified information of the same or higher category or by verification from the PIC-CVA 2/. When the requesting contractor's FCL status has been determined, his or her certification as to the proposed visitor's PCL status may be accepted. The visitor's identity shall be verified prior to any disclosure of classified information. If,

---

2/ The PIC-CVA address and telephone number are:

Defense Investigative Service
PIC-CVA
P.O. Box 1211
Baltimore, Maryland 21203-1211
(301) 633-4820

however, there is any question as to the validity of a visit request or identity of the visitor, appropriate confirmation shall be obtained from the contractor or UA activity that initiated the visit request.

b. The contractor shall establish such controls over the movement of approved visitors as are necessary to ensure that the visitors are only afforded access to classified information consistent with the authorized purpose of the visit. Particular care shall be taken to ensure that procedures for the control of Category 4 (foreign national) visitors are sufficient to prevent any access not provided for by the terms of the visit authorization. Such procedures shall provide for an escort while access is being afforded in accordance with the terms of the foreign national's visit authorization and when such a visitor is in areas where classified information may be accessible. The escort shall be a responsible, appropriately cleared employee who has been informed regarding the visitor's access limitations or restrictions on the visitor's movements.

c. Visitors shall be prohibited from making records of classified discussions and taking photographs in areas where classified information might be recorded on the film, without the express permission of the contractor being visited.

d. Classified material shall not be released to the visitor for removal from the contractor's facility, except as provided for by this manual.

39. Visitor Record.

a. The contractor shall maintain a record of all visitors to the facility for the purpose of having access to classified information. The record shall indicate: (i) the visitor's full name, (ii) the name of the contractor or activity he or she represents, and (iii) the date(s) of his or her arrival at and departure from the facility. The visitor record need not indicate whether the visitor actually did or did not gain access to classified information, but it must distinguish between classified and unclassified visits. Records of authorized visit requests for visits actually consummated shall be maintained by the contractor for a minimum of 2 years.

b. The contractor shall maintain a separate set of visitor records for NATO visits. A NATO visit shall be considered to be: (i) a visit by a person from a NATO country to a contractor in connection with precontract negotiations or contract performance on a NATO classified contract, (ii) a visit between a U.S. prime contractor and a subcontractor performing on a NATO classified contract, and (iii) other visits in which access to NATO classified information has been specifically authorized. Representatives of the CSO, whose requirement for access to NATO classified information is only incidental to the accomplishment of the security inspections at the contractor's facility, shall not be considered to be "NATO visitors" nor be required to enter their names on NATO visit records.

40. Long-Term Visitors. When employees of one contractor are temporarily stationed at a facility of another contractor, the security procedures of the facility visited will govern. However, when such visits are on a continuing

basis and it is found impractical for such visitors to comply with the security procedures of the host facility, the respective contractors shall prepare an agreement delineating their respective responsibilities and encompassing the procedures to be followed. This agreement must conform to the provisions of this manual and a copy shall be furnished to the CSO of the host contractor. The CSO of the host contractor is responsible for conducting periodic inspections to ensure that classified information in the possession of the visiting employees is properly safeguarded, and for notifying the host contractor of security deficiencies.

41. Visitor Categories and Procedures.

a. Category 1. This category applies: (i) when a contractual or prospective contractual relationship exists between contractors or between a contractor and a UA, and visits to a contractor by representatives of the GAO for auditing purposes, authorized representatives of the Department of Labor, and other agencies of the executive branch of the government when acting in their official capacities; (ii) to visits among prime contractors who are participating under government direction in contracts pertaining to research, development, or production of a weapon system; (iii) to employees of contractors producing items furnished to assembling contractors (GFP) for purposes pertaining to such assembly; and (iv) to employees of a cleared facility, which had previously been furnished a classified report directly by the contractor being visited under the specific terms of a contract (excluded from this category are facilities that receive only abstracts of classified reports or reports from sources other than the preparing contractor). Such visit requests will, in addition to the information required in paragraph 37, also contain a statement identifying the specific report that the visitor is authorized to discuss.

(1) The above visit requests will be submitted directly to the contractor to be visited.

(2) The contractor to be visited has approval authority, provided such visits meet the provisions of paragraph 37.

(3) The prime contractor or assembling contractor, as the case may be, may initiate visit requests for employees of a subcontractor or contractor supplying GFP, in accordance with paragraph 37, when he or she is in possession of the information required by paragraph 37d.

(4) Employees of a temporary help supplier working for contractors at their facilities shall be treated as regular employees of the using contractors for the purpose of security orientation in facility practices, procedures, and pertinent reports, while working under the contractors direction and control (see paragraphs 5u, v, ab, and 6b(1)). This action by the using contractor in no way relieves the temporary help supplier from complying with these and other requirements of this manual.

b. Category 2. This category applies to visits between contractors who have been granted FCL's, but do not have a contractual relationship, and visits that do not otherwise meet the requirements of Category 1.

(1) The requesting contractor will obtain in writing a verification of the visitor's need-to-know from his or her contracting officer or designee and include it with the visit request.

(2) The contractor to be visited will approve the request, if he or she desires the visit.

(3) The visiting contractor may substitute another cleared employee to make the visit without additional verification of the need-to-know, if this is acceptable to the contractor being visited. Information about the substitution shall be furnished to the contractor being visited, as required by paragraph 37d.

c. Category 3. This category applies to representatives or employees of the DOE and its contractors whose visits require access to other than RESTRICTED DATA.

(1) The activity requesting the visit will furnish the required information to the contracting officer of the UA whose information is involved, using DOE F 5631.20.

(2) If approved, the contracting officer will notify the contractor of the scheduled visit, including required information concerning the visit (DOE F 5631.20).

d. Category 4. This category applies to foreign representatives. Except as authorized in subparagraph 41d(8) below, visits to contractor facilities by foreign nationals (see paragraph 3ap) and persons acting as representatives of a foreign interest (see paragraph 3bw), hereafter referred to collectively as foreign representatives, must be officially sponsored by a foreign government. Foreign sponsorship is normally reflected in an official request for visit from the embassy of the nation concerned to the cognizant UA foreign disclosure office 3/. The cognizant UA may then sponsor, deny, or

---

3/ The Defense Intelligence Agency is responsible for processing requests to visit elements of the OSD, the Office of the Joint Chiefs of Staff (OJCS) the Unified and Specified Commands, the Defense Agencies, and activities administratively supported by the OSD. The following offices are responsible for processing other visit requests:

Department of the Army
Assistant Chief of Staff
for Intelligence
ATTN: Foreign Liaison
Directorate (DAMI-FL)
Washington, D.C. 20310

Department of the Air Force
International Affairs Division
Information Branch (CVAII)
Office of the Vice Chief of Staff
Washington, D.C. 20330

Department of the Navy
Foreign Disclosure and Policy
Control Branch
Office of Chief of Naval
Operations (OP-622E)
Washington, D.C. 20350

Defense Intelligence Agency
Foreign Liaison Branch (DI-4A)
Washington, D.C. 20301

elect not to sponsor the visit. UA sponsored visits shall not be used to avoid the licensing requirements of the ITAR published by the Department of State, or the Export Administration Regulations, published by the Department of Commerce. The contractor shall be responsible for ensuring that both sponsored and unsponsored visits by foreign representatives are effectively denied unauthorized access to: (i) classified information, (ii) unclassified technical data governed by the Export Administration Act, administered by the Secretary of Commerce, and the Arms Export Control Act, administered by the Secretary of State through the ITAR, and (iii) other unclassified information for which the DOE, NRC, or other government department or agency has prescribed dissemination limitations.

(1) Foreign nationals shall not be afforded access to classified information, unless specifically authorized in writing by a UA.

(2) The UA sponsorship of a visit is based on the existence of a specific or potential program or project with the foreign government concerned. UA notification of sponsorship will contain the level and scope of classified information authorized for disclosure (visual and/or oral only), as well as any limitations, and will be transmitted to the CSO for review and retransmittal to the contractor facility to be visited. Final acceptance of the visit will be subject to the concurrence of the contractor. The contractor shall notify the UA when the visit is not desired. The contractor may not change the level or scope of classified information to be released, or modify any limitations, without the approval of the UA that approved the visit.

(3) The contractor shall not inform the foreign representatives, or their employers, of the scope of access authorized or of the limitations imposed by the UA, nor shall the foreign representatives be induced to seek a higher access level than previously approved by the UA.

(4) The fact that a foreign representative may possess a PCL at a particular level does not automatically entitle the individual to receive U.S. classified information at that level.

(5) Prior to disclosure of classified information to foreign representatives, the contractor being visited shall advise such visitors of their responsibilities to safeguard the information to be disclosed. The contractor shall also inform the visitors that the information affects the national defense of the U.S. within the meaning of the espionage laws of the U.S., and that unauthorized disclosure violates international agreements and is harmful to the interests of national security.

(6) If the UA declines to sponsor a visit, a declination notice will be furnished to the requesting embassy with an information copy to the security office of the contractor facility(ies) to be visited. A copy of the visit request will accompany the declination notice. Lack of sponsorship does not equate to disapproval nor does it preclude accomplishment of the visit, provided the contractor has, or obtains, a munitions license for the specific technical information proposed for release, or the information is otherwise exempt from the licensing requirements of the ITAR. Unsponsored visits may be arranged between the foreign activity proposing the visit and the contractor. Disclosure of classified information during

unsponsored visits is prohibited: (i) without specific written authorization from the cognizant Military Department, or (ii) without a previously approved and current munitions license issued by the Department of State. It is the contractor's responsibility to consult applicable Department of State and Department of Commerce regulations to determine export licensing requirements or exceptions regarding the disclosure of unclassified technical data during visits by foreign representatives.

(7) In the event a UA denies a request to visit, the requesting embassy and the contractor(s) involved will be advised of the reasons(s) for it by means of the distribution channels prescribed in paragraph (6) above.

(8) The following rules apply to reciprocally cleared contractors:

(a) Visit requests involving U.S. citizen employees of reciprocally cleared contractors (see paragraph 31.3) that require access to classified information or unclassified information related to a classified program or project, and all visit requests involving foreign national employees of such firms, shall be processed to the UA foreign disclosure office having jurisdiction over the information involved. To reduce administrative burden and facilitate the timely conduct of visits associated with current or potential classified prime contractual or subcontractual relationships, contractors are encouraged to include as many activities to be visited as possible on each such request and propose that such visit request be approved on a recurring basis, preferably for the duration of the contract or subcontract involved. Copies of approved requests will be furnished by the cognizant UA foreign disclosure office to the requesting contractor and to each contractor and UA activity approved for visitation. All subsequent changes to the list of visitors may be communicated by the requesting contractor directly to the activities to be visited, ATTN: Security Officer, making reference to the pertinent approved visit request on file. However, requests to visit activities not previously approved must be submitted separately to the cognizant foreign disclosure office for approval.

(b) Visits by U.S. citizen employees for unclassified commercial purposes may be arranged directly with the security office of the contractor or UA activity to be visited.

e. Category 5. This is a special purpose category which is to be applied in rare situations and only with the written authorization of the UA whose classified information is involved. It pertains to persons who do not qualify under any of the other categories, and whose visits to a contractor's facility are considered necessary and essential by the contractor who states in writing that the visitor cannot be denied access to classified information by escort or other security measures. Only U.S. citizens are eligible to make visits in this category. Under no condition, shall a visitor in this category be permitted physical custody or personal possession of classified information. Access to classified information at the TOP SECRET level is prohibited and shall not be authorized.

(1) Contractors are required to deny access to classified information by escorting visitors or by other security measures. However, under certain circumstances, contractors may be unable to effectively prevent aural and or visual access to classified information by a visitor.

In these situations, the contractor shall advise the UA and obtain authorization before allowing the visit to take place by submitting the following information to the UA:

(a) Name of the visitor, date and place of birth.

(b) Name of company or agency of employment and address. (If self-employed, so indicate.)

(c) Purpose and justification for the visit in sufficient detail to allow the UA to determine the necessity for the visit. Numbers or names of programs, projects, or contracts which are involved, should be provided for identification purposes. Level of the classified information involved must be specified.

(d) A complete and detailed explanation of the reasons escort or other security measures cannot be provided by the contractor effectively prevent aural and or visual access to classified information by the visitor.

(e) Date of proposed visit and anticipated duration of time required for the visit.

(f) Completed DD Form 48 and FD Form 258, as specified in paragraph 26, or forms as directed by the UA. The contractor to be visited shall act as a sponsor instead of an employer in the completion of forms and shall act as a witness wherever required on the forms. Verification of U.S. citizenship shall be accomplished in the same manner as required by paragraph 5ae.

(2) Visit renewals may be authorized at the discretion of the UA.

(3) Personnel security clearances under the DISP are not authorized for a visitor in this category.

42. Visits Involving Access to RESTRICTED DATA.

a. Visits to a DoD or NASA contractor by a DoD or NASA representative or contractor shall be processed as prescribed in paragraph 37.

b. Visits to a DoD or NASA contractor by representatives of UA's, other than DoD and NASA and their contractors, require prior approval of the DOE. The DOE F 5631.20 shall reflect this approval in part B of the form. Contractors submitting visit requests in this category shall, after certifying to the clearance status of the proposed visitor(s) in part A of the DOE F 5631.20, forward the form to the contracting officer for certification of the visitor's need-to-know and further processing, in accordance with the UA's regulations. The contractor receiving a visit request in this category shall ensure that the required certifications have been made and that the visit has received DOE approval.

c. Visits to a UA contractor, other than to a DoD or NASA contractor by representatives of the contracting UA and between a prime contractor and his or her subcontractor on such a UA contract, shall be processed as prescribed in paragraph 41.

d. Visits to a UA contractor, other than to a DoD or NASA contractor by representatives of UA's other than the contracting UA and by contractors other than under a prime-subcontractual relationship, require prior approval of the DOE and shall be processed in the manner prescribed in paragraph b above.

Part 2. VISITS TO USER AGENCY ACTIVITIES

43. General Rules -- In Addition to Paragraph 37.

a. Contractors shall comply with any requests received from the Commander or Head of UA activities for additional information needed in the processing of visit requests.

b. The contractor is encouraged at the time of the initial visit to request approval for subsequent visits within a period of 12 months, when necessary and consistent with the purpose of the initial visit. Arrangements for continuing visits will be made between the contractor and the Commander or Head of the UA activity. Final approval is the prerogative of the Commander or Head of the UA activity.

c. Visits to DoD or NASA activities by DoD or NASA contractors, involving access to RESTRICTED DATA, shall be processed as prescribed in paragraph 42a. Visits to other UA's involving access to RESTRICTED DATA shall be processed in the manner prescribed in paragraph 42b.

d. Contractor employees shall comply with written regulations and operating instructions issued by UA activities concerning visitors to such activities.

44. Visits to User Agency Activities in the United States.

a. Visits to Field Activities. Contractors desiring to have an employee or consultant visit a UA activity involving access to classified information shall address a request in writing to the Commander or Head of the activity to be visited. Visit requests shall be accompanied by a statement from the contracting officer that the release of classified information is required in connection with a specified classified contract or program. (Visit requests normally will be sent via the contracting officer.)

b. Visits to UA Activities in the Washington, D.C. Area. Requests to visit offices of headquarters activities of the UA's in the Washington, D.C. area shall be submitted in writing and addressed to the specific office to be visited. Whenever possible, the exact code number, division, branch, and so on, of the activity or office to be visited shall be included in the address of the request. Visit requests shall be accompanied by a statement from the contracting officer that the release of classified information is required in connection with a specified classified contract or program. (Visit requests normally will be sent via the contracting officer.)

c. As an exception to paragraphs a and b above, a visit request may be submitted directly to the activity or office to be visited without a statement from the contracting officer, when the classified information to be disclosed and the determination as to the contractor's need for such access is known to be a responsibility of the activity or office to be visited. This exception does not apply to visits involving access to classified intelligence information as set forth in paragraph e below.

d. The contractor's request shall contain the information specified in paragraph 37d.

e. If a contractor contemplates discussion or viewing of classified intelligence in the custody of a UA activity, the contractor's visit request shall be forwarded in all cases to the contracting officer of the UA activity authorized to release classified intelligence to contractors for the required need-to-know verification and routing to the UA to be visited. In addition to the information specified in paragraph 37d, the visit request shall contain the following:

(1) the contractor's certification that: (i) access to classified intelligence is required for contract performance, and (ii) the contract is a classified contract (see paragraph 3i), and

(2) sufficient additional information concerning classified intelligence required to permit the agency or activity receiving the visit request to assess:

(a) applicability of available classified intelligence to the contractor's needs, and

(b) whether available intelligence may be released to the contractor without permission of the originator and/or sanitation of the material.

45. Visits to User Agency Activities Outside the United States. This paragraph is applicable when a contractor desires to have an employee make a classified or unclassified visit to a UA activity outside the U.S. The information required by paragraph 37d shall be furnished for the visits enumerated in this paragraph.

a. Contractor Sponsored Visits. A contractor shall process a request for his or her employee to visit a UA activity outside the U.S. through DISCO to the UA activity concerned, if the visit is on the initiative of the contractor. The Commander or Head of the activity to be visited will notify the contractor of the approval or disapproval of the visit request. (See paragraph 50 for an employee based in Europe.)

b. UA Sponsored Visits. A visit request for a contractor employee sponsored by a UA and traveling on the UA's orders will be processed by the UA, in accordance with the regulations of such agency. The traveler's orders shall reflect the traveler's level of security clearance, if required, in connection with the travel. The contractor shall submit the request for such visit directly to the UA activity concerned.

Part 3. VISITS TO GOVERNMENT ACTIVITIES OTHER THAN USER AGENCIES

46. Visits to DOE Installations or DOE Contractors. Requests for visits to DOE installations or to DOE contractors, which will require access to DOE classified information, shall be prepared utilizing DOE F 5631.20. (Copies of this form may be obtained from any DOE installation.) In addition to completing the appropriate portions of the DOE F 5631.20, the contractor (usually the FSO) shall include in the first block of the form immediately after the personnel clearance data, a certification of the prospective visitor's PCL. The DOE F 5631.20 shall then be forwarded, for the required official certification, to the contracting officer of the UA who signed the DD Form 254 that was issued in connection with the contract for which the DOE classified information is required.

47. Visits to Activities Other Than DOE. Requests for visits to government activities, other than UA's and the DOE, which involve the release of classified information to such activities in connection with a UA contract, require the approval of the contracting officer and, if the classified information to be released includes RESTRICTED DATA, the approval of the DOE. Such requests shall be submitted by the contractor to his or her contracting officer who will process the request. The contractor shall provide evidence of the fact that the activity to be visited had either requested the proposed visit or consented to the contractor's request for the visit. In addition, a statement shall be included explaining: (i) the purpose of the visit in detail, (ii) a description of the classified information to be divulged during the visit either to or by the activity being visited, and (iii) the direct or indirect effect the visit may have on the performance of the classified contract involved.

Part 4. VISITS TO FOREIGN GOVERNMENTS AND ACTIVITIES

48. General.

a. Contractor visits to foreign governments or activities or to international bodies fall into three categories.

(1) The first includes visits that involve the disclosure of U.S. classified information:

(a) in connection with a government-to-government agreement to furnish U.S. military equipment to the foreign government (that is, the purchase of the equipment is under a U.S., not a foreign government contract);

(b) in connection with exploratory sales visits, precontract negotiations, or contract performance, other than those covered under paragraph (a) above (that is, the purchase of the U.S. military equipment or services when and if consummated will be or is under a foreign government contract); or

(c) in connection with U.S. Government presentations to foreign governments and international pact organizations, when the U.S. Government has requested the contractor's participation.

(2) The second includes visits that do not involve disclosure of U.S. classified information, but where the foreign government or activity requires a U.S. security assurance on the visitor:

(a) which involve disclosure of unclassified technical data on the "U.S. Munitions List;" or

(b) which will not involve disclosure of technical data on the "U.S. Munitions List."

(3) The third includes visits on a commercial basis (that is, the visits do not involve disclosure of U.S. classified information and do not require a U.S. security assurance on the visitor). These visits may or may not involve disclosure of unclassified data on the "U.S. Munitions List." Visits in this category are not processed under the provisions of this manual. However, the contractor is responsible for compliance with the ITAR and for obtaining a State Department export license or letter, if required.

b. The following information concerning the requirements of the ITAR is furnished for the guidance of the contractor:

(1) Disclosure of classified information, in connection with visits in the category described in paragraphs a(1)(a) and (c) above, does not require an export license.

(2) Except as specified in paragraph (3) below, disclosure of unclassified technical data related to "U.S. Munitions List" items requires an export license.

(3) An export license is not required if the visit has been approved on an unclassified basis by the UA concerned, and (i) the technical data to be disclosed is information covered by a manufacturing license or technical assistance agreement approved by the Department of State, or (ii) the technical data to be disclosed is exempt from the provision of the ITAR.

c. Requests for visits to foreign governments or activities shall be processed only for an employee who is the subject of an LOC. Contractor-issued CONFIDENTIAL clearances are not valid for such visits.

d. Visit requests shall be processed as follows:

(1) Visit requests in the categories described in paragraphs a(1)(b) and a(2)(a) and (b) above shall be processed by the contractor through DISCO.

(2) Visits in the categories described in paragraphs a(1)(a) and (c) above shall be processed by the contractor, in accordance with the regulations of the UA that is dealing with the foreign government. The contractor shall certify visit clearance information directly to the UA

concerned. If the UA is unable to process such requests, they will so endorse the contractor's request and refer it to DISCO for processing. Such endorsement will constitute approval of the visit and reference to an export license will not normally be required on the visit request.

e. Visit requests processed through DISCO shall be submitted in duplicate with one extra copy for each additional country to be visited, and shall contain the information required in paragraph 37d, as well as the proposed visitor's passport or identification card number, and date and place of issuance. In addition, the contractor shall specify the category of visit that is involved (see paragraph a above) and, for a visit of the type described in paragraphs a(1)(b) or a(2)(a) above, will certify the export license number and license expiration date within the visit request. For visits to the Swiss Government and contractor facilities, the legal residence address of each visitor must also be shown.

49. Processing Time. Visit requests should be received by DISCO at least 45 days in advance of the proposed travel date for all countries and U.S. overseas commands. Exceptions are for travel to Switzerland, which requires 70 days advance notice. Requests for visits in France must be for specific dates, as France will not approve visits for indefinite periods.

50. Use of OISI. If the U.S. contractor employee making the visit is based in the Far East or in Europe, or in an adjacent country, the visit request may be submitted through OISI rather than through DISCO. The information required in paragraph 48e shall be included with the request. The OISI will verify the proposed visitor's security status. In addition to furnishing a copy of the export license or letter, when required in accordance with paragraph 48e, the contractor is responsible for compliance with the ITAR, if applicable, in the same manner as though the visit were arranged through DISCO.

Part 5. VISITS IN CONNECTION WITH BILATERAL INDUSTRIAL SECURITY AGREEMENTS AND NATO VISITS PROCEDURES

51. Visits in Connection With Bilateral Industrial Security Agreements.

a. The following procedures apply to visits pertaining to precontract negotiations or contract performance under approved bilateral agreements involving a foreign classified contract in the U.S. or a U.S. classified contract in a foreign country.

(1) Authorization for visitors or those visited to have access to classified information shall be limited to that necessary for official purposes in connection with precontract negotiations or contract performance. When requested, the authority to visit the facility of the prime contractor may include authorization to have access to or to disclose classified information at the facility of a subcontractor engaged in performance of work in connection with the same contract.

(2) A list may be developed to indicate those individuals who are authorized to visit the facility for extended periods of time, not to exceed 6 months, as may be necessary in the performance of the contract. This authorization may be renewed for additional periods of 6 months as may be necessary in the performance of the contract.

(3) Visits shall be approved only for persons possessing U.S. Government granted security clearances.

b. U.S. contractor visits in connection with foreign classified contracts shall be processed in accordance with the provisions of paragraph 48.

c. Representatives of foreign governments visiting U.S. activities shall be processed as Category 4 visitors, in accordance with paragraph 41d, if U.S. classified information is involved in the foreign government's contract. If only foreign classified information is involved, the visit shall be processed by DISCO.

52. NATO Visit Procedures. The following visitor control procedures apply to a NATO precontract negotiation or to a NATO contract awarded to a U.S. contractor by a NATO government other than the U.S., a contractor of such NATO country, or a NATO international body:

a. Visits by Representatives of a U.S. Contractor to the NATO Contracting Officer, a NATO Management Office, or a Contractor of a NATO Country Other Than the U.S. The visit request, in quadruplicate, will be directed through DISCO to the NATO contracting office or to the NATO management office and will be processed together with a Certificate of Security Clearance (see paragraph 55). The Certificate of Security Clearance shall indicate whether or not the visitor has received a NATO security briefing. Whenever possible, the NATO security briefing will be accomplished prior to the submission of the visit request and the certificate will state so. When this is not practical, the visit request will include a statement as to when and by whom the NATO security briefing will be conducted. (OISI-(E) offices in Brussels, Belgium, or in Mannheim, Germany, will conduct NATO briefings when requested.) The visit request shall include the information specified in paragraph 37d, the visitor's passport or identity card number, date and place of issuance, and the NATO contract or program on which he or she is engaged.

b. Visits by Representatives of NATO Contracting Officer, a NATO Management Office, or of a Contractor of a NATO Country to the U.S. Contractor. Such requests shall be processed by the NATO activity concerned as a Category 4 visit (see paragraph 41d) through the appropriate UA activity. Such visit requests will contain the information specified in paragraph a above.

c. Visits in Connection with NATO Contracts by Representatives of a U.S. Contractor to Another U.S. Contractor in the U.S.

(1) Such visits shall be processed as Category 1 visits (see paragraph 41a), if both contractors are performing on the same NATO contract in a prime contractor to subcontractor or subcontractor to subcontractor relationship. A statement on NATO security briefing shall be included in the visit request.

(2) If no contractual relationship exists between the contractors, the visit request shall be processed as a Category 2 visit (see paragraph 41b) requiring the approval of the NATO contracting officer whose information is involved. Supporting information on NATO briefing and the Certificate of

Security Clearance shall be included in such visit requests. The visit request, together with two copies of the Certificate of Security Clearance, will be processed through DISCO to the NATO Contracting Officer.

d. Recurring Visits. Subsequent visits shall be processed in accordance with paragraph 37f. Authorization for subsequent visits shall not exceed a period of 12 months, but may be subject to renewal for succeeding periods of 12 months, if required (see paragraph 53b for NPLO visit requests).

53. NATO Production Logistics Organization (NPLO) Programs Clearance and Visit Procedures. Clearance and visit control procedures in effect for contractors performing on specific NPLO programs are different from other NATO visit procedures. Current NPLO programs are HAWK, F-104G, NAMSA, and NISCO. As an aid to simplifying visit procedures, it is necessary to establish the visiting contractor employee's clearance in connection with a specific NPLO program. This may be accomplished prior to the initial or concurrently with the request for such visit.

a. Initial Visits.

(1) The visit request, in quadruplicate, will be directed through DISCO to the NPLO Management Office with a copy to the NATO activity to be visited and will be processed together with a Certificate of Security Clearance (see paragraph 55). The visit request shall include the information specified in paragraph 37d, the visitor's passport or identity card number, date and place of issuance, and the NPLO program with which he or she is concerned.

(2) The DISCO will forward the visit request to the NPLO Management Office, which will inform appropriate NATO and foreign activities of its approval or disapproval.

(3) The Certificate of Security Clearance will be forwarded by DISCO to the NATO Office of Security, Industrial Security Section, for recording and dissemination to the NATO member countries and NPLO Management Offices concerned.

(4) In case of urgency when a Certificate of Security Clearance has not been forwarded to the NATO Office of Security, Industrial Security Section, in advance, DISCO will attach a copy of the Certificate of Security Clearance to the visit request for transmission to the NPLO Management Office.

b. Recurring Visits. If the initial visit is approved, subsequent visits, not to exceed 6 months to the same NPLO activity for the same U.S. contractor employee, will be processed by the U.S. contractor directly to the NPLO activity to be visited. That activity will notify the contractor of the approval of the visit. These subsequent visit requests will contain the information required by paragraph 37d and will include the visitor's passport or identity card number, and date and place of issuance.

54. Records of NATO Visits. The contractor shall keep a separate set of visitor records for NATO visitors containing the information specified in paragraph 39.

55. Certificate of Security Clearance.

a. A standard format Certificate of Security Clearance has been adopted for use within the NATO community in connection with visits from one NATO country to another, or to a NATO office, agency, command, or to or between contractors when a visit will involve access to NATO classified information.

b. The Certificate of Security Clearance shall be completed on plain bond paper by the contractor for his or her employees desiring to make a visit, and submitted in duplicate for certification to DISCO. The employee's name shall be listed in the following order: last name, first name, middle name.

c. This certificate shall be sent sufficiently in advance by the contractor through DISCO so as to ensure receipt by the foreign officials of the NATO offices, agencies, commands, or contractors before arrival. In exceptional circumstances, the information required by the certificate may be supplied by other means of communication, but must be confirmed in writing. Normally, a copy of this certificate should not be given to the traveler.

(Sample)

DEFENSE INDUSTRIAL SECURITY
CLEARANCE OFFICE

Certificate of Security Clearance

(Authorizing Access to NATO Classified Information)

Issued by ______________________________

Date and place of issue ______________________________

____

Valid until ______________________________

(If issued to an individual, this certificate should be returned to the granting authority on the termination of the mission for which issued.)

This certifies that ______________________________
(Last name, first name, middle name)

Date of birth ______________________________
Place of birth ______________________________
Nationality ______________________________
Where employed ______________________________
Program(s) ______________________________
Holder of passport/identity card No. ______________________________
Issued at ______________________________
Military rank and number ______________________________
(where applicable) has been cleared for access to information classified up to and including ______________________________
in accordance with current NATO Security Regulations.
(Has)(Has not) received a NATO Security briefing.
Date of briefing: __________

____
Signature and Title of Granting Authority
(seal or stamp)

Section VI. SUBCONTRACTORS, VENDORS, AND SUPPLIERS

56. Application to Subcontractors. The provisions of this manual apply to subcontractors, vendors, or suppliers of prime contractors (hereafter referred to as a subcontractor). A subcontractor shall submit requests through the prime contractor to the contracting officer for an authorization or approval requiring action by the contracting officer under the provisions of this manual. However, if any such request is clearly encompassed in an authorization previously given in writing to the prime contractor by the contracting officer, in relation to a specific contract, the prime contractor, acting within the scope of such authorization, may approve or disapprove such request. Requests involving release of U.S. classified information to foreign subcontractors must be forwarded to the UA for authorization.

57. Application to Sub-Subcontractors. For the purposes of this manual, each subcontractor shall be considered as a prime contractor in relation to his or her subcontractors.

58. Determination of Clearance Status.

a. The prime contractor shall determine from the Personnel Investigations Center (PIC)-Clearance Verifications Activity (CVA), mailing address:

Defense Investigative Service
PIC-CVA
P.O. Box 1211
Baltimore, MD 21203-1211
Telephone Number (301) 633-4820

that the prospective subcontractor has been granted an appropriate FCL prior to disclosure of any classified information, unless there is an existing contractual relationship between the parties involving classified information of the same or higher category. (An FCL is not prima facie evidence that a facility has the capability to physically safeguard classified material.) If physical possession of any classified material is to be granted to the prospective subcontractor, the procedures outlined in paragraph 59 shall be followed.

b. If the prospective subcontractor does not have an appropriate FCL, the prime contractor may request the CSO of the subcontractor to initiate clearance action. The term "prospective subcontractor," as used herein, means a subcontractor whose services are required for the performance of an existing classified contract or subcontract. Requests will include, as a minimum, the full name, address and telephone number of the requester; the full name, address, and telephone number of a contact at the facility to be cleared; the level of clearance and safeguarding capability required; and full justification for the request.

c. Requests to process a prospective subcontractor for an FCL must be based on a bona fide procurement need for the prospective subcontractor to have access to, or possession of, classified information during contract activity, such as preparation of bids and proposals and precontract negotiations, the performance of the subcontract, and all aspects of post-contract activity. Requesting cleared contractors shall allow sufficient lead time in connection with the award of a classified subcontract to enable an uncleared bidder to be processed for the necessary FCL. When the FCL cannot be granted in sufficient time to qualify the prospective subcontractor for participation in the current contract activity, the CSO will continue the clearance processing action to qualify the prospective subcontractor for future classified contract consideration provided:

(1) The delay in processing the FCL was not occasioned by a lack of cooperation on the part of the prospective subcontractor;

(2) Future classified contract negotiations may likely occur within 12 months; and

(3) There is a reasonable likelihood the contractor may be awarded a classified subcontract.

59. Safeguarding Ability.

a. Prime contractors, having complied with paragraph 58a, shall obtain written approval from the contracting officer, or his or her designated representative, prior to the disclosure of TOP SECRET information to prospective subcontractors.

b. Prime contractors, having complied with paragraph 58a, shall determine that prospective subcontractors meet the requirements of this manual for safeguarding TOP SECRET, SECRET, and CONFIDENTAL material prior to granting physical possession of such material to prospective subcontractors. (This determination may be made at the same time as the FCL determination is made under paragraph 58a.) 1/ Such determination shall be based on the following:

(1) the prime contractor's knowledge of the ability of the prospective subcontractor to safeguard adequately the material to be released and produced under the subcontract based on a current contractual relationship involving classified material of the same or higher category as that to be released or produced under the new subcontract, or

(2) the written authorization of the PIC-CVA or, if appropriate, the CSO of the prospective subcontractor. In this connection, the prime contractor shall provide the PIC-CVA or the CSO of the prospective subcontractor with available information, such as description, quantity, end-item, and classification of information related to the proposed subcontract and any other factors, in order to assist the PIC-CVA or the CSO in determining whether the prospective subcontractor meets the safeguarding requirements of this manual.

1/ Under the following circumstances, the PIC-CVA will not be able to respond and requesters shall make inquiries to the appropriate CSO: (i) requests involving the transfer of material that would require more than two cubic feet of storage, (ii) requests involving commercial carriers under the provision of paragraph 17c5(c), ISM, and (iii) requests for certification of security clearance and safeguarding ability to the DTIC.

(3) The PIC-CVA or, if appropriate, the CSO of the prospective subcontractor shall advise the prime contractor in writing that the prospective subcontractor is or is not physically equipped to safeguard the classified material involved. When necessary action is taken by the prospective subcontractor to provide adequate safeguards, the CSO of the prospective subcontractor shall immediately inform the prime contractor.

(4) Verifications may be requested from the PIC-CVA by telephone or letter and from the CSO, if appropriate, by message, telephone, or letter. Should the foregoing verifications be requested via telephone, oral confirmation will (normally) be immediately provided. In any event, under normal circumstances written confirmation will be furnished to the requester within 5 working days from receipt of inquiry, regardless of mode. Unless otherwise notified (superseded) in writing by the PIC-CVA or the CSO, if appropriate, each verification furnished in accordance with this paragraph shall remain valid for a period of 1 calendar year from the date of issuance.

(5) Clearance status and safeguarding capabilities of facilities shall be obtained only when a specific procurement need exists.

60. Classification Guidance.

a. Prime contractors have a requirement to inform prospective subcontractors of the category of classification to be assigned the various elements in a subcontract, RFQ, RFP, IFB, or other solicitation. The prime contractor in preparing the DD Form 254 for his or her subcontracts may extract pertinent data from the DD Form 254 pertaining to the prime contract. The DD Form 254 prepared by the prime contractor shall be submitted to the official shown in item 16e of the prime contract's DD Form 254 for approval and distribution, or authorization and instructions for distribution, by the prime contractor. In the absence of exceptional circumstances which clearly support classification, the DD Form 254 will not be classified. If classified supplements are required as part of the security guidance, they shall be identified in item 15 of the DD Form 254 and forwarded by separate correspondence. Classified information shall be so furnished after verifying clearance status and safeguarding ability, in compliance with paragraphs 58 and 59. The provisions of this paragraph do not waive the requirements of paragraph 62.

b. After selection of a subcontractor, the prime contractor shall prepare a DD Form 254 for the subcontract and shall request the official designated in item 16e of the DD Form 254 for the prime contract to approve and sign the DD Form 254 for the subcontract and to make the required distribution. However, with the agreement of the contracting activity, the prime contractor may accomplish the required distribution of the approved DD Form 254. The distribution schedule of the DD Form 254 is included as paragraph 61.

c. When the prime contractor receives a revised DD Form 254 providing additional guidance or a change in guidance, he or she shall prepare a revised DD Form 254 for each subcontractor whose DD Form 254 requires a related change. An ACO/PCO authenticating signature and distribution, or instructions for distribution, of the contractor's DD Form 254 are required. When prime contractors receive notices that reviews have reaffirmed their existing guidance, or receive revised DD Forms 254 that do not require related changes in any subcontractors' DD Forms 254, they shall promptly give written notices of reaffirmation of guidance to each subcontractor involved. This notice of reaffirmation to subcontractors does not require ACO/PCO authenticating signature. Instead, a true copy of the notice of reaffirmation received by the prime contractor, or, when applicable, a true copy of pages 1 and 2 of the revised DD Form 254 received by the prime contractor, annotated by the prime contractor with the statement, "This revised DD Form 254 does not affect your current DD Form 254 dated ________________________," will suffice. In either of the above cases, a signed transmittal letter from the prime contractor shall be attached. Distribution of this written notice of reaffirmation to subcontractors shall be in accordance with paragraph b above. With respect to an MFO, the HOF shall provide the guidance for the revised DD Form 254, or the written notice of reaffirmation of the existing guidance described above, as applicable, to each of its operating facilities affected by the revised guidance or involved in the notice, as the case may be.

d. The prime contractor will receive from the UA a DD Form 254 for each classified item of GFP or GFE issued or authorized for purchase, when such material is not covered by the classification specification issued with the contract. The contractor shall furnish a DD Form 254 providing the classification specification necessary for each of the subcontractors requiring use of classified GFP or GFE in connection with their contracts or negotiations for contracts with the prime contractor.

e. A new DD Form 254 is not required for a follow-on contract or subcontract when the procurement is of a recurring nature, or the end item is not changed and there is no change in the security classification requirements of the contract. However, a copy of the currently valid DD Form 254 for the preceding subcontract shall be furnished and distributed with the follow-on subcontract and annotated in items 3 and 4 to show the contract number and date of the follow-on prime contract and subcontract. Item 6 will also be completed, as appropriate.

f. There is no authorized substitute for the DD Form 254. There are exceptional conditions in which a prime contractor has a serious time limitation in preparing his or her response to a RFP, IFB, or similar solicitation to a UA. In such cases the prime contractor, concurrent with dispatching the DD Form 254 for official U.S. Government approval and signature, may supply an unofficial copy of the same guidance to a prospective subcontractor for the latter's use pending receipt of the approved and signed DD Form 254.

g. A single DD Form 254 may be used to provide the classification specification for an open-end or call type subcontract, except when the individual call, purchase order, or request for services or products requires a different classification specification from that provided for the overall subcontract.

h. The following special provisions are applicable to service, graphic arts, research, or commercial carrier classified contracts:

(1) A DD Form 254, which specifies the highest level of classification involved, but does not provide detailed classification guidance, will be issued under the following circumstances:

(a) The total requirement of the contract is the performance of a service, all of which takes place at a cleared contractor's facility or U.S. Government activity which has and makes available, for use by the contractor performing the service, a currently valid Contract Security Classification Specification, which includes complete guidance for the service to be performed. In such cases, item 15 of the DD Form 254 will be annotated: "Using contractor or activity will furnish complete classification guidance for the service to be performed. The highest level of classification for the contract is (TOP SECRET, SECRET, or CONFIDENTIAL). Contract performance is restricted to (name of facility or location)."

(b) The contractor has no performance requirement involving actual knowledge of, generation, or production of classified information, but has only a requirement to be physically present in an area where classified information is located. Examples include, but are not limited to, contracts calling for guard, IDS, alternate storage, or equipment maintenance services. In these cases, item 15 of the DD Form 254 will be annotated: "Actual knowledge of, generation, or production of classified information is NOT REQUIRED. This document serves as written notice of the letting of a classified service contract. The highest level of classification for the contract is (TOP SECRET, SECRET, or CONFIDENTIAL)."

(c) The contract requirement is limited to graphic arts reproduction and classification markings appearing on the material to be reproduced. These classification markings constitute the required Contract Security Classification Specification. In these cases, item 15 of the DD Form 254 will be annotated: "Reproduction service only. The highest level of classification for the contract is (TOP SECRET, SECRET, or CONFIDENTIAL). Classification markings on material to be reproduced specify the required security guidance."

(2) When a cleared commercial carrier enters into a classified service subcontract with a cleared facility, within the meaning of paragraph (1)(b) above, the carrier, serving as a prime contractor for such purpose, will issue a DD Form 254 to that cleared facility. In any such case, the requirements of paragraphs (1)(b) above and (3) below will apply.

(3) In each of the cases described in paragraphs (1) and (2) above, if a subcontract at any tier is involved, the DD Form 254 for the subcontract will not require authentication by the signature of an ACO/PCO. Instead, the contractor who is the principal prime, or who serves as a prime contractor in relation to a subcontractor in the particular case, will complete and sign item 16. Further, in all cases distribution of the DD Form 254 will be made to the subcontractor involved, his or her CSO, and the contract administration office(s), if designated, of the immediate prime contractor and subcontractor involved.

(4) Where a contract involves research services requiring detailed classification guidance, but it is too early to determine these detailed requirements, item 15 of the DD Form 254 will be annotated: "This is a research contract. The highest level of classification for the contract as a whole is (TOP SECRET, SECRET, or CONFIDENTIAL). A revised DD Form 254 will be issued as soon as possible, to provide detailed security classification guidance."

i. In the case of a subcontract, which is expected to require access only to classified reference material (see paragraph 3bt), an original DD Form 254 will be issued to describe the highest category or various categories of classification of such material to which access will be required and to provide other instructions, as appropriate; for example, the protection of information extracted from such material. Classification guidance concerning reference material is the responsibility of the department or agency having classification jurisdiction over such material at the time it was prepared, or of the current successor in interest of that department or agency. When the prime contractor requires classification guidance for reference material in order to prepare a DD Form 254 for the subcontractor, or for other reasons and needs assistance in identifying the responsible department or agency, he or she shall, by direct communication, seek assistance from the following:

(1) The secondary distribution source from which the material was received. Examples of secondary distribution sources are: DTIC, Alexandria, Virginia 22314 and its field extensions; DoD Information Analysis Centers; and the Redstone Scientific Information Center, U.S. Army Missile Command, Redstone Arsenal, Alabama 35808.

(2) The UA contracting office last involved with the contractor concerning the subject matter of the material.

(3) If unsuccessful in identifying the responsible department or agency by communication with (1) and (2) above, the contractor shall seek assistance from:

(a) the UA which awarded the prime contract, or

(b) the Director for Information Security, OUSD(P).

61. Required Distribution. Original, final, and revised DD Forms 254, supplements, attachments, and written confirmation of existing classification specifications are to be distributed as follows 2/:

2/ Reflect the distribution in the "Required Distribution" block of the DD Form 254. For SENSITIVE COMPARTMENTED INFORMATION contracts, distribution of the DD Form 254 and attachments will be as prescribed by the procuring contracting agency concerned.

a. For prime contracts:
   (1) Prime contractor
   (2) CSO of prime contractor
   (3) Appropriate ACO
   (4) Quality assurance representative
   (5) Official identified in item 12b, DD Form 254
   (6) Others as necessary

b. For subcontractors:
   (1) Prime contractor
   (2) Appropriate ACO
   (3) Subcontractor
   (4) CSO of subcontractor
   (5) Quality assurance representative
   (6) Official identified in Item 12b, DD Form 254
   (7) Others as necessary

c. For sub-subcontracts:
   (1) Prime contractor
   (2) Appropriate ACO
   (3) Subcontractor
   (4) Sub-subcontractor
   (5) CSO sub-subcontractor
   (6) Quality assurance representative
   (7) Official identified in Item 12b, DD Form 254
   (8) Others as necessary

d. For solicitations (IFB, RFQ, RFP), distribution of DD Form 254 for IFB, RFQ, or RFP, will be the same as for the prime contract, subcontract, or sub-subcontract to which the solicitation is related, except that none is to be sent to the quality assurance representative.

62. Notification of Selection. The prime contractor shall immediately furnish in writing to the contracting officer, or his or her designated representative, the names and addresses of each of the subcontractors to be engaged on classified work under a prime contract, and the highest classification of information that shall be released or developed thereunder.

63. Unsatisfactory Security Conditions. If notified by a CSO of unsatisfactory security conditions within a subcontractor's facility, contractors shall follow the instructions they receive from the contracting officer relative to what action, if any, should be taken in order to safeguard classified material relating to their subcontract.

64. Disposition of Classified Information. The subcontractor shall destroy classified material, as provided by paragraph 19, unless the prime contractor requests return or authorizes retention. However, the prime contractor shall obtain the approval of the contracting officer, or his or her designated representative, authorizing a subcontractor to retain classified information.

65. Subcontracting With Foreign Industry.

a. The U.S. has entered into bilateral security agreements with several foreign governments to establish the intent of both parties to protect each others classified information. The U.S. negotiates two basic types of security agreements, the General Security of Information Agreement (GSOIA) and the Industrial Security Protocol. The CSO should be contacted concerning whether a particular country has entered into either type of bilateral agreement.

(1) The General Security of Information Agreement (GSOIA). The GSOIA is a government-to-government agreement, negotiated through diplomatic channels. It states, in substance, that each party to the agreement will afford to the classified information provided by the other the degree of security protection afforded it by the releasing government. It contains provisions concerning the use of each government's information, third party transfers, and proprietary rights. It specifies that transfers of information will be on a government-to-government basis. It provides that both parties agree to report any compromise, or possible compromise, of classified information furnished by the other party. Moreover, the GSOIA states that both parties will permit visits by security experts of the other party for the purpose of conducting reciprocal security surveys. The purpose of such surveys is to determine whether the foreign government has the capability to protect U.S. classified information in a manner that is substantially equivalent to the protection afforded to it by the U.S.

(2) The Industrial Security Protocol. The Industrial Security Protocol is negotiated by the DoD as an annex to the GSOIA, with those foreign governments with which DoD has entered into coproduction, codevelopment, and/or reciprocal procurement arrangements, involving industry. It includes provisions for clearance of facilities and personnel, the handling and transmission of classified material, and procedures for visits.

b. The above-cited security agreements apply only when a contract, subcontract, or other such government approved arrangement, is awarded to a foreign or U.S. contractor by or on behalf of the U.S. Government or the signatory foreign government, as applicable. They do not apply in the case of an industry-to-industry arrangement, unless it is in furtherance of a documented government-to-government cooperative program, for example, a coproduction memorandum of understanding. In such instances, the government-to-government arrangement will stipulate that all classified military information approved for release under the program will be safeguarded, in accordance with the applicable GSOIA and Industrial Security Protocol. If such agreements do not exist with the foreign government concerned, the necessary security provisions are incorporated in the documentation establishing the government-to-government program. Consequently, subcontracts, which require the release of U.S. classified military information. may be awarded to foreign industry only when: (i) the subcontract is in furtherance of a specific government-to-government arrangement, or (ii) assurances are obtained through government channels that the government of the country in which the foreign industry resides will assume responsibility for ensuring the security protection of the U.S. classified information involved. All such subcontracts require the approval of the UA having jurisdiction over the classified information involved.

66. Subcontracts Arising From Foreign Classified Contracts. Unless specifically prohibited in the contract, a U.S. contractor awarded a foreign classified contract by a government with which the DoD has entered into a bilateral industrial security agreement may subcontract within the U.S., in accordance with the provisions of this manual, within the country of the contracting foreign government, in accordance with instructions furnished by the designated agency of that government, through the Deputy Director (Industrial Security), HQ DIS. In addition, a U.S. contractor may subcontract within any other country only with the permission of, and under conditions agreed to by, the contracting government, and the government of the country of the subcontractor. These conditions shall be furnished to the contractor through the Deputy Director (Industrial Security), HQ DIS. In those cases where U.S. classified information is involved in the subcontract, the contractor or foreign government, shall, prior to its release to the foreign government, obtain an export letter/license authorization from the Department of State or specific approval of the U.S. UA that originated the information.

Section VII. CONSULTANTS

67. General. PCL and/or FCL requirements for self-employed consultants to UA activities and contractors shall be determined in accordance with this section. In all cases, self-employed consultants shall have valid PCL's issued in accordance with the requirements of this manual. Consultants are not eligible for access to classified information outside the U.S. and its trust territories and possessions, unless in official travel status of not more than 90 days in any 12-month period. Consulting firms and Type B Consultants shall be processed for an FCL. As a general rule, however, self-employed consultants will not require an FCL, regardless of the business structure involved. The CSO will provide advice regarding the need for a particular consulting firm to be cleared.

68. Consultant -- Type A. The consultant does not access or possess classified material except at the using contractor's cleared facility or on the premises of a UA activity, when employed as a consultant by the UA, or while on visits as authorized under section V. All requirements of this manual apply to the consultant who, for security administration purposes only, shall be considered to be an employee of the UA.

a. Should an FCL for the consultant not be required, the using contractor or UA activity and the consultant shall jointly execute a certificate as follows:

(1) Except in connection with authorized visits: classified material shall not be possessed by the consultant off the premises of the using contractor or UA; the using contractor or UA shall not furnish classified material to the consultant at any other location than the premises of the using contractor or UA, and performance of the consulting services by the consultant shall be accomplished at the activity of the using contractor or UA; and classification guidance will be provided by the using contractor or UA.

(2) The consultant shall not disclose classified information to unauthorized persons.

(3) The using contractor or UA shall brief the consultant as to the security controls and procedures applicable to the consultant's performance.

b. One copy of such certificate shall be furnished by the using contractor to his or her CSO. In the case of a consultant to a UA activity, the certificate shall be retained by the Commander or Head of that activity.

c. The consultant shall complete the forms required by paragraph 26. These forms shall be submitted to DISCO by the UA activity or the contractor for which the consulting service is to be performed. Each application for clearance shall be accompanied by a copy of the certificate prescribed by paragraph a above. The LOC shall be issued to the using contractor or UA activity, as appropriate.

69. Consultant -- Type B. The consultant possesses classified material at his or her place of business or residence, the consultant having full responsibility for security of the classified material.

a. An FCL is required for the consultant to cover the premises at which he or she will possess the classified material and perform the consulting services.

b. Consultants of this type shall be considered to be prime contractors to the UA activity, or subcontractors to the using contractor.

c. The provisions of this manual pertaining to contractors or subcontractors, as appropriate, shall apply.

70. Consultant -- Type C. Consultants possess classified material at their regular employer's cleared facility, the consultants and their employer having agreed as to their respective responsibilities for security of the classified material. The clearance status and safeguarding ability of the consultants' regular employer shall be obtained from the PIC-CVA, prior to the disclosure or release of any classified information to the consultant.

a. No requirement exists for a separate FCL for the consultant (including execution of the DD Form 441 and the DD Form 441s) or to have an existing FCL raised, provided that the employing facility, and the employee who is acting as a consultant to another contractor or to a UA activity, are both cleared for access to at least the category of classified information as that to which the consultant will require access, and provided the employing facility and the employee jointly execute a letter agreement to safeguard classified information for an employee performing consultant services (see appendix I, paragraph V) by which the employing facility and the employee agree to the following:

(1) Both agree to place classified material, which the consultant-employee must have in his or her possession, into the employing facility's accountability system.

(2) Both agree to incorporate procedures in the employing facility's SPP, which prohibit the dissemination of the classified material within the facility, except that appropriately cleared personnel of the facility may be designated in writing on a strict need-to-know basis to provide the consulting employee clerical, destruction, and reproduction services necessary to his or her performance as a consultant.

(3) Both agree to furnish the employee, who is acting as a consultant, a storage container, so that the classified material may be stored under his or her control. Access to the storage container shall be limited to the employee who is acting as a consultant and the minimum number of employees designated in accordance with paragraph (2) above, which are essential to support the consultant.

(4) Both agree to advise its CSO immediately on any change in the consultant's status as an employee of the facility.

b. One copy of the letter agreement described in paragraph a above, shall be furnished by the employing facility to its CSO, and one copy to the contractor or UA employing the consultant.

c. In the event it is necessary to raise the consultant's PCL to a higher level (not above that of the employing facility), the consultant shall complete the forms required by paragraph 26 and submit them through the employing facility to DISCO with a copy of the letter agreement prescribed in paragraph a above. (If required to be cleared to a higher level than that of the employing facility, the consultant shall be processed for a separate FCL, in accordance with paragraph 69, and required to maintain a security program fully independent of that of his or her employer.)

71. Consultants to User Agencies Employed Under Civil Service Procedures. Security clearances for persons employed as consultants to UA's under civil service procedures normally will be issued under the separate regulations of the UA concerned. However, UA's may process such a consultant for a PCL and/or an FCL under the provisions of paragraph 68-70, when deemed desirable.

Section VIII. PARENT-SUBSIDIARY AND MULTIPLE FACILITY ORGANIZATIONS

72. Parent-Subsidiary Relationships.

a. When a parent-subsidiary relationship exists between two companies, the parent company must have an FCL of the same or higher classification level as the subsidiary company, unless by formal action of its board of directors or similar executive body: (i) it is excluded from access to all classified information held by the subsidiary company, or (ii) it is excluded from access to classified information held by the subsidiary company, which
is of a higher classification level than the parent company's FCL. How- *
ever, if the parent company is under FOCI and the FOCI cannot be negated *
or reduced to acceptable levels, exclusion action may not be taken. In *
such circumstances, the subsidiary company is ineligible for an FCL. *
Exceptions to this rule can be made pursuant to certain bilateral security *
agreements and approved freight forwarders. (Consult the CSO for details.) *
Each exclusion action shall be made a matter of record in the minutes of the executive body of both the parent company and the subsidiary company. Two copies of both sets of minutes shall be furnished to the CSO of each cleared subsidiary company, along with a copy of the DD Form 441s, executed independently by the excluded parent company and the subsidiary company. In addition, when officers or directors of a subsidiary hold similar positions with the excluded parent company, they shall execute one of the following certificates, as appropriate: (i) "I understand that the (name of parent company) is not cleared for access to classified information and I certify that I shall not disclose classified information to the (name of parent company) or any of its agents, regardless of my official business or personal association therewith," or (ii) "I understand that (appropriate classification level) is the highest level of classified information which may be disclosed to the (name of parent company) or any of its agents, regardless of my official business or personal association therewith." Official notice of the execution of each such certificate shall be made a matter of record in the minutes of the executive body of the subsidiary company and two copies of the minutes shall be furnished to the CSO of the subsidiary. Two copies of each certificate, executed in accordance with the requirements of this paragraph, shall be furnished to the CSO of the subsidiary.

b. Interchange of classified information and visits between a parent and its subsidiaries, or between the subsidiaries, shall be accomplished in the same manner as an interchange between a prime contractor and a subcontractor. However, in the case of a classified contract awarded to a subsidiary, the subsidiary, as necessary in the performance of the contract, may release classified information to the parent, when required, provided the parent company has an appropriate FCL and safeguarding ability. Moreover, where the parent organization is owned or controlled by a foreign interest, the U.S. subsidiary shall not release U.S. classified information to the parent, except with the express written authority of the contracting UA. In such cases visits between the subsidiary and the parent shall be considered as Category 1 visits, as defined in paragraph 41a. Neither the subsidiary nor the parent may release or disclose classified information, pertaining to the contract of the subsidiary, to other subsidiaries of the parent without specific approval of the contracting officer or his or her designated representative, or unless within the provisions for exceptions set forth in paragraph 5x.

c. In case the parent corporation or its subsidiaries have cleared facilities which are collocated with each other (occupying the same office space or located side by side), the collocated facilities may request CSO approval of a formal written agreement between the facilities to utilize common security services for: (i) personnel security administration, (ii) document control (to include storage), (iii) reproduction, (iv) visitor control, and (v) other similar administrative services. In all cases, the agreement shall be incorporated into the SPP (or appropriate supplement to an SPP) applicable to the facilities involved. The proposed SPP shall be submitted to the CSO as part of the request. The SPP shall establish workable security procedures and clearly fix responsibility for security administration within the collocated facilities. The procedures shall be structured (for example, separate accountability systems) to ensure that the need-to-know principles outlined in the previous paragraph are not violated. One FSO shall be designated for all facilities; the designee shall be considered an OODEP of these facilities and shall require a concurrent clearance at each facility. Appropriately authorized (cleared with a need-to-know) personnel rendering security services shall be designated in the agreement by job title to provide the specific services agreed to. Additionally, procedures may be incorporated into the SPP whereby a machine run or other roster (for example, record of clearance) may be used in lieu of a visit letter, provided such records are maintained in a current status at all times. When combined, the SPP and the roster shall provide the essential information required in paragraph 37d.

73. Multiple Facility Organizations (MFO). The home office facility (HOF) of an MFO is responsible for ensuring compliance with the terms of the Security Agreement (DD Form 441) and with the security requirements for each classified contract being performed by all elements and locations within the MFO, to include all cleared and uncleared subordinate locations at which cleared personnel are located. A copy of the DD Form 441, with Appendage (DD Form 441-1) shall be furnished to each facility listed in the Appendage and to each CSO concerned. The HOF shall have an FCL at the same, or higher, level as any cleared facility within the MFO. The following procedures and requirements are applicable to an MFO, unless an exception has been granted to the HOF of a freight forwarder. * * *

a. Standard Practice Procedure (SPP). The SPP of an MFO shall include security instructions which provide the controls necessary to protect classified information within the organization. As a minimum, the SPP shall include instructions for (i) maintaining clearance records and briefings, (ii) the transmission of classified information between the cleared facilities, and (iii) for visits of employees between the cleared facilities 1/. Within each cleared facility, the SPP shall then be adapted, as necessary, to meet the local conditions. When a contractor elects to have the LOC's issued to the HOF or to a PMF, the subordinate cleared facility remains responsible for complying with all provisions of this manual applicable to a cleared facility unless specific allowable exceptions are identified in the HOF/PMF, and the cleared subordinate facility's

---

1/ Visits by cleared employees between facilities of an MFO are considered Category 1 visits and paragraph 41a applies.

approved SPP. If cleared employees are employed or physically located at uncleared locations, the SPP for the HOF/PMF that holds their PCLs shall reflect that the HOF/PMF, as appropriate, is responsible for personnel security administration.

b. Interchange of Classified Information. Classified information may be interchanged among the cleared facilities of the MFO when essential for contract negotiations and performance. The releasing facility is responsible for determining that the proposed recipient facility has an appropriate facility security clearance and the necessary safeguarding capability.

c. Security Classification Guidance. Security classification guidance, commensurate with the involvement of the receiving facility, shall be provided by the releasing facility. This guidance does not have to be a DD Form 254 but it shall be written guidance tailored to the performance of the receiving facility and shall include the prime contract number. A copy of the DD Form 254 received by the releasing facility may be used, if applicable, or guidance may be extracted from a DD Form 254 or from an appropriate classification guide(s). Regardless of the form of the guidance, it may be signed by the contractor. A copy shall be provided to the CSO of the receiving facility. If only classified documents are provided to another facility, and the documents themselves provide the necessary guidance, no further classification guidance need be provided. If the receiving facility's performance will involve any special security requirements, such as, special access briefings, prohibitions against subcontracting, reproduction, or transmission, it is essential that appropriate guidance be provided to the facility and its CSO.

d. MFO/PMF Security Clearances. Normally a cleared employee's PCL is required to be at the same, or at a lower level, as that of the facility's security clearance where the employee is principally employed and the employee's LOC is retained by that facility. However, there are exceptions allowed to these requirements in an MFO or PMF with specifically defined geographical or functional areas for subordinate cleared or uncleared locations where cleared employees are physically located. The contractor may, with the prior approval of the CSO, elect to have all LOC's issued to the HOF, or to one or more PMF's. Prior to requesting DISCO to send LOC's to a HOF or PMF, the contractor shall develop procedures for inclusion in its SPP and submit it to the CSO of the HOF or the PMF for review. As a part of the SPP, the contractor shall submit an initial listing of the name and location of subordinate facilities (cleared and uncleared) for which the HOF and/or PMF will hold the LOC's. The SPP shall specify the security responsibilities of these subordinate facilities and must have CSO approval prior to requesting DISCO to issue LOC's to the HOF or PMF.

e. Personnel Security Administration Responsibilities in an MFO. The following requirements are applicable when cleared employees are employed or physically located at uncleared locations:

(1) the contractor shall designate a properly cleared management official at the uncleared location who shall:

(a) conduct recurring security briefings for all cleared employees;

(b) provide written confirmation of the briefings to the HOF or PMF that is holding the LOC's;

(c) implement the reporting requirements of paragraph 6 concerning all cleared employees at the uncleared locations and furnish the reports to the appropriate HOF/PMF for further submittal as required; and

(d) in situations when there is no suitably cleared management official available at the uncleared location, the recurring security briefings may be conducted by the FSO of the HOF/PMF or their appropriate cleared representative. These briefings may be conducted during visits by the FSO to the uncleared locations or during visits by the employees to the cleared facility. The FSO shall retain a record of the briefings until after the next security inspection by the CSO. Such procedures shall be set forth, as appropriate, in the HOF/PMF SPP.

(2) The HOF or PMF shall provide appropriate reports to its CSO listing all uncleared locations where cleared employees are located.

(3) All classified visit requests shall be dispatched by the HOF or PMF.

(4) Procedures applicable to briefing cleared employees who are assigned to locations outside the U.S. are contained in paragraph 97.

74. Temporary Help Suppliers.

a. General. A temporary help supplier is a subcontractor who dispatches personnel on his or her payroll to perform work on the premises of the using contractor or UA (see paragraph 5ab). A temporary help supplier and his or her field, branch, or associate offices having a valid parent-subsidiary or MFO relationship are covered in paragraphs 72 and 73 respectively. The following paragraphs are concerned with:

(1) a temporary help supply licensor (hereinafter referred to as the licensor) who grants licenses or franchises to other individuals or firms to use the name, administrative support, methods of operation, or style of the licensor in a specific geographic area; and

(2) a license or franchise holder (hereinafter referred to as a licensee) who owns and operates a legal entity separate and distinct from the licensor, and is licensed or franchised to do business under the name, method of operation, or style of the licensor.

b. Where the temporary help personnel are actually employees, and on the payroll, of the licensee, the licensee may be granted an FCL as provided for in this manual.

best copy available

c. Where the temporary help personnel are employees, and on the payroll, of the licensor, normally there would be no valid basis for the licensee to be granted an FCL. As an alternative, an FCL may be granted in the name of the licensor at the address of the licensee, if there is a valid requirement for employees of the licensor to have access to classified information at a contractor facility or UA activity, provided that:

(1) the licensor has an FCL at its HOF; and

(2) an employee of the licensor located on the premises of the licensee is appointed as FSO for the licensor; or

(3) an employer-employee relationship is established between the licensor and at least one or more employees of the licensee through execution of a separate written agreement between the parties, or by the insertion of a clause in the franchise or license agreement. The agreement or clause shall specifically provide that, for a consideration, one or more employees of the licensee will act as FSO for the licensor in the territory covered by the license or franchise. One signed copy or certified true copy of the agreement or clause shall be furnished by the licensor to the CSO concerned.

d. If the provisions of paragraphs c(1) and (2), or c(1) and (3), above are followed, an FCL may be granted to the licensor at the address of the licensee. This location will, for industrial security purposes, be considered as an operating facility of an MFO. Among other things, the SPP of the operating facility shall specify the functions and responsibilities of the FSO and the procedures for:

(1) processing PCL's including the granting of company CONFIDENTIAL clearances by the FSO;

(2) accomplishing the requirements of paragraphs 5 and 6 which relate to its (temporary help) personnel; and

(3) processing visit requests dispatching its temporary help personnel to the using contractor's facility as Category 1 visits (see paragraph 5ab and 41a).

e. When a licensee has a license or franchise agreement with more than one licensor, an FCL may be issued in the name of each licensor. Similarly, if a contractor is engaged in a business which requires an FCL in connection with such business and, in addition, is a licensee for a temporary help supplier, an FCL may be issued in his or her own firm's name and one in the name of the licensor.

f. Temporary help suppliers shall not engage Type A Consultants for dispatch elsewhere. Each temporary help supplier shall be the user of the services offered by the Type A Consultant it sponsors for a PCL.

Section IX. SENSITIVE COMPARTMENTED INFORMATION AND COMSEC INFORMATION

75. SENSITIVE COMPARTMENTED INFORMATION.

a. The provisions of this manual apply to research, development, and production of SENSITIVE COMPARTMENTED INFORMATION (SCI). In addition, special security requirements supplementing this manual will be prescribed by the contracting department for SCI contracts, except that, for SCI contracts awarded by military department procurement activities for the NSA, the NSA will prescribe the special security requirements.

b. In the case of SCI contracts awarded by military department procurement activities for the NSA, the NSA shall be responsible for exercising security controls over the contract.

c. In the case of SCI contracts awarded by and for a military department or DoD Agency, an activity designated by the contracting military department or DoD Agency shall be responsible for exercising security controls over the contract.

d. Access to SCI will be granted to contractor employees requiring access by the activity designated to exercise security controls over the contract as provided above.

e. Denial or revocation of authorization for access to SCI is not appealable.

76. COMSEC Information. The contractor shall protect COMSEC information in accordance with the requirements of the DoD 5220.22-S (CSISM).

Section X. GRAPHIC ARTS

77. Special Requirements for Graphic Arts. This section of the manual provides specific security measures for the safeguarding of classified information by the graphic arts industry. The security measures apply whether the work is performed by the prime contractor on his or her premises or subcontracted to a graphic arts facility.

78. Production Control Records. While the production control records remain with the classified job to which they relate, they shall be: (i) plainly and conspicuously marked or stamped at the top and bottom with the same classification as the material being produced, or (ii) unless the production control record itself contains classified information, covered over with a cover sheet conspicuously marked or stamped at the top and bottom with the same classification as the material being produced. In either case, the additional markings required by paragraph 11b(8) shall be applied, as appropriate. Production control records or cover sheets shall be marked with a notation indicating that they are unclassified when separated from the classified material being produced, unless they contain or have attached thereto classified information. The contractor may, at his or her discretion, use the production control records as the records required by paragraphs 12 and 18, provided they contain the required information and are retained for the period of time specified in paragraph 12.

79. Area Controls -- Additional Requirements. During the layout, composition, platemaking, presswork, and bindery stages of the production of classified material, controls shall be established to deny unauthorized personnel access to the immediate area in which such work is being performed. In the event the safeguarding requirements prescribed in paragraph 16 are insufficient for this purpose, such areas shall be designated as restricted areas and shall be controlled in accordance with the provisions of paragraph 34b. Additional requirements are as follows:

a. Pressrooms. While the press is being made ready or being run, the press itself shall be identified and marked the same as the classified information being run. The press shall remain so identified until the run has been completed and all classified material removed. Marking and identification of the press is not required for press runs of short duration, provided the run is completed prior to the end of the workday. Plates, blankets, chases, and the like, need not be removed from the press at close of working hours, when the press run is incomplete, provided the area meets the requirements of paragraph 34a(3).

b. Composition Areas. Linecasting (for example, intertype and linotype) and photocomposition machines shall be identified and marked the same as the classified information being set in type, except for jobs of short duration completed prior to the end of the working day. Slugs (that is, lines cast on a linecasting machine), coded tapes, ribbons, negatives, and so on, need not be removed from the machines at the close of the workday when the composition is not completed, provided the area meets the requirements of paragraph 34a(3).

c. Bindery Area. Bindery areas shall be secured by the same method as pressroom areas.

d. Darkrooms. Admittance to all film processing units shall be restricted to cleared personnel who are assigned to the particular job or jobs involving classified information.

e. Proofreading Areas. Proofreading areas shall be controlled by physical barriers capable of preventing visual or audio access and entrance by unauthorized persons.

f. Shipping Entrances. Shipping entrances shall be secured when classified information is in the area. Loading and unloading operations shall be performed under the supervision of a cleared employee of the contractor.

80. Special Conditions.

a. Overruns. All assembled copies of printed material not spoiled during a printing operation, which are in excess of the number of copies ordered, shall be designated as overruns. Overruns shall be held to a minimum. An exact count of the overruns shall be maintained and they shall be accounted for as prescribed in paragraph 12. Overruns shall be transmitted to the customer with the balance of the job or promptly destroyed in compliance with the provisions of paragraph 19a through e [1].

b. Proofs. A record shall be kept of the number and disposition of proofs. Galley or page proofs approved by the customer shall be retained until the product is delivered, and shall be returned to the customer along with the original manuscripts [1].

c. Waste Disposal. The contractor shall provide properly identified waste containers at each production point at which waste, spoilage, trimmings, or cuttings accumulate. Waste shall include paper stock used for press make-ready, spoilage during running, printed copies spoiled during bindery make-ready, or excess copies of individual pages that are not to be assembled to form a complete product. Waste containers shall be adequately safeguarded and the waste promptly destroyed, in accordance with paragraph 19f. Waste shall not be retained in production areas during nonworking hours.

d. Return of Samples. All graphic arts samples (that is, classified material furnished by the customer for reproduction) shall be returned to the customer immediately after the completion of the work [1].

---

[1] Where the classified production has been accomplished on the premises of the contractor, as opposed to being done by a graphic arts subcontractor, the disposition of overruns, proofs, samples, and other material, except for waste used in the production of the job, may be delayed until the completion or termination of the contract concerned.

e. Bulk Shipment. Graphic arts products that are shipped in bulk in double containers will be stacked in the inner container face up. A cover sheet shall be placed on top of the material before sealing the inner container. The contractor shall maintain a record of the quantity shipped in each container, and when copies are serially numbered, the contractor shall number the inner containers, and the record shall show which serial numbers were packed in each container. Such records shall be incorporated into the control station records maintained in accordance with paragraph 12. The classification markings and, if appropriate, the notations prescribed in paragraph 11b(8), shall be applied on all outside surfaces of the inner container. Outer containers shall be sealed by wire stapling or by tape, so that tampering will be evident. No markings shall be made on the outer containers, which will in any way indicate that the package contains classified material. Address labels will be placed on the top surface of both containers, and receipts will be placed inside the inner container.

f. Materials Used in Production.

(1) All materials used in production, which contain classified information (that is, negative flats, layouts, masters, dummies, vellums, stencils, composition tapes, proofs, tympan sheets, negatives, type, plates, and so on), shall be safeguarded, in accordance with paragraphs 14 and 16, and immediately after completion of the work, destroyed in accordance with paragraph 81, or returned to the customer along with the job on which they were used 1/ (see paragraph 12f for accountability requirements).

(2) Rubber blankets, after use in a classified production, may be reused on classified and unclassified production, provided they are properly washed and safeguarded, in accordance with paragraph 16. The rubber blankets shall be identified as required in paragraph 11c and the classification shall at all times reflect the highest category of classified information for which the rubber blanket has been used (see paragraph 12f for accountability requirements). When no longer serviceable, or reuse is not desired, rubber blankets used for classified productions shall be destroyed as prescribed in paragraph 19c.

(3) Plates and other than rubber blankets used on a classified production shall not be reused, and shall be destroyed as prescribed in paragraph 81. A contractor is not authorized to turn over classified plates to a subcontractor for the sole purpose of regraining such plates. Moreover, the regraining of plates shall not be considered as an authorized method of destruction under paragraph 81.

(4) "Rollers" and other parts of presses, which retain impressions of classified information during the printing stages, shall be cleaned to remove the classified information on completion of the run.

81. Destruction -- Special Requirements. Classified material used in the reproduction process shall be destroyed, in accordance with paragraph 19c, except that:

a. classified information on metal foundry and wooden type shall be considered as having been destroyed when the type is redistributed in the type case; and

b. classified information on glass negatives shall be destroyed by dissolving the emulsion or by pulverizing.

82. Mailing Lists.

a. Classified. When a mailing list used for the distribution of unclassified material is classified, the material shall be protected as though classified (markings not required), until separated from the classified mailing list.

b. Unclassified. When a mailing list used for the distribution of classified material is unclassified, the list shall be protected as though classified (markings not required), until separated from the classified material.

c. Related Material. When classified mailing lists are prepared or maintained by a contractor, all material which retains an impression of the addresses, such as carbons, addressing plates, identification strips, and verification lists, shall be classified and safeguarded accordingly.

Section XI. NATO INFORMATION

83. Application. This section of the manual provides for the additional security measures that have been established for the safeguarding of NATO classified information. The provisions contained in this section supplement the provisions of sections I through X of this manual. These additional security measures apply whether the NATO classified information is in the possession of the prime contractor or in the possession of his or her subcontractor(s). The provisions of this section do not apply to U.S. documents which contain NATO information (see paragraphs 11b(8)f and 11e(2)).

84. Authority. The requirements of this section reflect the security procedures established by the U.S. Security Authority for NATO for the safeguarding of NATO classified information in the possession of U.S. industry.

85. Supervision and Orientation Requirements.

a. The FSO is responsible for supervising and directing security measures for safeguarding NATO classified information.

b. In addition to the clearance record required by paragraph 28, the contractor shall maintain a separate record of all employees located at the facility who have been authorized access to NATO classified information.

c. The contractor shall notify all employees who will have access to NATO classified information of the following:

(1) The term "NATO classified information" used in this section applies to classified information circulated within and by NATO, including information released by member nations into the NATO security system, as well as information originated in the organization itself. However, classified information contributed by a member nation remains the property of the originating nation, even though it is circulated in a document belonging to NATO.

(2) The marking "NATO" on a document is used to signify that the document is the property of NATO. This marking will be applied to all copies of documents classified SECRET, CONFIDENTIAL, and RESTRICTED that are circulated within NATO. The marking of "COSMIC" also signifies that the document is the property of NATO, and is applied exclusively to all copies of TOP SECRET documents circulated within NATO.

(3) COSMIC TOP SECRET documents, NATO SECRET documents, and NATO CONFIDENTIAL documents shall be protected according to the rules in other sections for TOP SECRET, SECRET, and CONFIDENTIAL material and the additional rules prescribed in this section. NATO documents marked "RESTRICTED," which are furnished to the contractor, shall be marked and protected as prescribed in paragraph 11e.

d. The contractor shall bring to the attention of all employees, who will be authorized access to NATO classified information, their continuing individual responsibilities for safeguarding NATO classified information. They shall also be advised that when they are in other NATO countries they may be subject to the laws of those countries that pertain to the handling of classified information. When access to COSMIC TOP SECRET information is involved, employees shall sign certificates to the effect that they have been briefed on their responsibilities for safeguarding COSMIC TOP SECRET information.

86. Security Clearances.

a. A final PCL granted by DoD for a U.S. citizen is valid for access to NATO information of the same or lesser security classification, provided the individual has been given a security briefing, in accordance with paragraph 85d above. U.S. citizens who require access to NATO RESTRICTED information must have a need-to-know for the information but a security clearance is not required.

b. An LAA granted to a foreign national is not valid for access to NATO classified information; however, foreign nationals of a NATO member nation employed by a cleared U.S. contractor may be authorized access to NATO classified information provided that: (i) there is a written request from the contractor with an expressed need for the foreign national to have access to NATO information, (ii) the written approval of the NATO contracting officer has been obtained, and (iii) a NATO Security Clearance Certificate is obtained by DISCO from the individual's home country. The approval for NATO access will only be granted in connection with performance on a NATO contract.

c. Application for a NATO Security Clearance Certificate for a foreign national of a NATO member country shall be made by the U.S. contractor as provided below:

(1) The contractor shall submit to DISCO an executed DD Form 49 and two completed FD Forms 258. The words 'NATO SECURITY CLEARANCE CERTIFICATE' shall be placed in bold letters above the "Signature of Employer or Designated Representative" block of the DD Form 49.

(2) Requests for NATO Certificates for foreign nationals must be accompanied by the NATO contracting officer's written consent for the individual to have access, and the contractor's letter which identifies the applicant, national identity number, (if any), permanent home and mailing addresses, telephone number and passport number. The letter shall also include the specific reason for the NATO clearance, the level of clearance required, the social security number of the applicant, and the period of time for which access is required.

d. The contractor will receive a letter from DISCO to certify that the applicant's National Security Authority has authorized NATO access. This letter will serve as the LOC for access to NATO information. This letter will also indicate an expiration date for the NATO clearance

certificate. If no request for renewal is received at DISCO prior to the *
expiration date, a cancellation letter will be sent to the contractor and *
the pertinent National Security Authority. *

e. NATO certificates granted under the provisions of this section *
are valid only for access to NATO classified information associated with *
the NATO classified contractor or program for which it was requested. It *
is not valid for U.S. classified information, other foreign classified *
information, or NATO ATOMAL information. *

87. Reproduction, Preparation, and Marking.

a. Requirements in paragraph 18 and section X apply equally to the reproduction of NATO classified documents. In the case of COSMIC TOP SECRET information, reproduction requests shall be forwarded to the Central U.S. Registry (CUSR) for authorization. (Address: Chief, CUSR, Room 1B889, The Pentagon, Washington, D.C. 20310).

b. Except for COSMIC TOP SECRET material, special permission is not needed to include references to, extracts from, or paraphrases of NATO classified documents in other documents, which the contractor must prepare in performance of the NATO contract.

c. Requirements in paragraph 11 apply equally to the marking of NATO classified documents. A SECRET, CONFIDENTIAL, or RESTRICTED document that is reproduced from a NATO document shall be marked NATO at the top and bottom, in addition to the classification markings. A TOP SECRET document that is reproduced from a NATO document shall be marked COSMIC at the top and bottom, in addition to the TOP SECRET marking.

d. When NATO classified information is included in other documents, the NATO classified information shall be identified within the document by marking each paragraph with the appropriate NATO marking. Moreover, a statement will be included on the cover or first page, as applicable, that the document contains NATO classified information.

88. Transmission of NATO Material.

a. When NATO SECRET or CONFIDENTIAL material is prepared for transmission and an inner container is required by paragraph 17a, that container shall be marked NATO, in addition to the classification marking. When transmitting NATO TOP SECRET material the inner container shall be marked "COSMIC TOP SECRET," in addition to the "TOP SECRET."

b. The transmission of NATO classified information within the U.S. shall be in accordance with the procedures set forth in paragraphs 17b, c, and d, except that the minimum requirement for mailing NATO CONFIDENTAL information is U.S. Registered Mail.

c. Documents classified NATO RESTRICTED shall be packaged and mailed *
as U.S. First Class Mail and may be single wrapped. To ensure continuous *
control by U.S. personnel, transmission outside the U.S. and its territor- *
ies shall be by U.S. Postal Service, First Class Mail, using an APO/FPO *
address. Geographical addresses and international mail channels shall not *
be used. *

d. All NATO classified information furnished to a U.S. contractor in connection with a U.S. classified contract shall be transmitted to destinations outside the U.S. only with the authority of the contracting officer. If such information is to be returned to the U.S., approval of the contracting officer is not required.

(1) COSMIC TOP SECRET transmitted to or from the U.S. shall be transmitted to the Chief, CUSR, Room 1B889, The Pentagon, Washington, D.C. 20310, by one of the methods authorized by paragraph 17b for forwarding to the intended destination.

(2) NATO SECRET and NATO CONFIDENTIAL information transmitted to or from the U.S. shall be transmitted by the contractor via one of the means authorized in paragraph 17e, with the following exceptions: Canadian postal channels cannot be used to transmit NATO classified material; information transmitted to a NATO activity outside the U.S. shall be transmitted to an appropriate U.S. activity for forwarding to the NATO activity; NATO classified information coming to the U.S. shall be transmitted through an appropriate U.S. Government activity to the U.S. contractor.

e. NATO classified information furnished to a U.S. contractor in connection with a NATO command or agency, or NATO member nation's classified contract or project, shall be transmitted to destinations outside the U.S. only with the authority of the contracting officer. Hand-carrying of NATO CONFIDENTIAL and SECRET material across international borders may be authorized by the CSO, provided an urgent situation exists, such as a need exists for personnel to travel on short notice, time does not allow documents to be sent ahead by approved secure means, and copies cannot be made available locally at the travelers destination. The contractor shall notify the CSO of the urgent situation, which necessitates the need to hand-carry the material, and request the CSO to approve this exception. The CSO may issue a NATO "Courier Certificate" for the appropriate cleared contractor employee to hand-carry the NATO material, provided: (i) the employee is to be routed via U.S. flag or other NATO member nation air carrier, (ii) the route taken to the NATO country destination is not to be over a Designated country, nor will the aircraft land in a Designated country, and (iii) if travel will be taken by surface means, it will not be through a non-NATO member nation. The CSO will affix a proper stamp to the certificate, as well as the authorizing signature of a designated official of the CSO. *

(1) Pre-Travel Procedures. Prior to issuing a NATO "Courier Certificate," the contractor shall ensure that the following steps are taken:

(a) All reasonable steps have been taken to make other arrangements for delivery of the NATO material to its destination: that is, the existing availability of the information at the destination.

(b) The employee designated to carry the material is cleared to the level of the classification of the information to be hand-carried.

(c) The employee has been provided the location of secure storage facilities on the premises of NATO commands or agencies, or a NATO member nation including U.S. Government installations.

(d) A suitable container, which can be retained in the employee's possession at all times, will be used to secure the material in transit.

(e) The package is properly sealed, and an accounting has been made of the contents.

(f) The details of itinerary with a specimen of the seal used will be completed by the government.

(g) The employee has been properly briefed by the U.S. Government on his or her responsibilities, as well as on emergency safeguarding procedures and has read and signed the NATO "Briefing Certificate." The briefing certificate shall be retained for 1 year.

(2) Packaging. Each package to be hand-carried shall contain only NATO classified material through NATO SECRET. The FSO or designee shall personally inspect each proposed shipment to verify its contents. The material shall be packaged, as provided for in paragraph 17, and shall bear an appropriate seal on the exterior of the package. The seal shall also be affixed to the details of itinerary column adjacent to each stage of the trip listed on the itinerary sheet. The seal will be placed under the line "Specimen of Seal Used." The name and address on the package must be that of the sender and addressee, if different from that of the employee hand-carrying the material.

(3) Seals. The contractor will have a NATO, U.S. Government, or company seal affixed by a representative of the CSO or other authorized U.S. Government official approved by the CSO.

(4) Custody. In the event it is necessary to store the package, as provided for in 1.c. above, a receipt shall be obtained for the material. On arrival at the destination and delivery of the package, a receipt shall also be obtained. It will be the responsibility of the recipient to sign the receipt for the contents of the package. The receipt for the contents of the package may be returned to the sender by mail or turned over to the contractor employee who hand-carried the package.

(5) Customs Search. If an official insists that the package be opened regardless of the NATO "Courier Certificate" and the employee's claim to exemption, the employee should open the package, but only to the extent that the customs official can confirm that NATO classified documents are contained therein. The employee shall request that the customs official both reseal the package in his or her presence and provide written evidence of the incident. The courier shall make a full report of the incident to the FSO on returning to the facility.

(6) Return Travel. Should the employee be authorized to carry the same documents on the return journey, the NATO "Courier Certificate" shall so state and an accounting shall be made by the contractor on the employee's return. In the event a NATO command or agency, or a NATO member nation or one of its contractors, wishes to have the employee hand-carry NATO classified material back to the U.S., the employee will follow the procedures established by the requesting NATO command, agency, government activity, or contractor. Procedures for hand-carrying NATO classified material across international borders are similar, since they are based on requirements established for all member nations by NATO.

e. All NATO classified bulky material, of any category, shall be sent through channels established by the CSO on instructions from the Deputy Director (Industrial Security), HQ DIS.

89. Functions of the Contracting Officer.

a. When a U.S. contractor enters into precontract negotiations involving NATO classified information with a U.S. contracting officer, the contractor shall obtain his/her instructions from the contracting officer concerned, as prescribed in this manual.

b. When a U.S. contractor enters into precontract negotiations with a NATO government other than the U.S., a contractor of such NATO country, or a NATO international body requiring that the contractor have possession and access to NATO classified information in the U.S., the U.S. contractor shall request the necessary instructions from the contracting officer of such NATO country or international body.

90. NATO Reporting Requirements. The contractor shall immediately report, through the CSO to the Chief CUSR, Room 1B889, The Pentagon, Washington, D.C. 20310, receipt of COSMIC TOP SECRET information from a source outside the U.S., when the information has not been transmitted via the CUSR. A copy of the report shall be sent to the Deputy Director (Industrial Security), HQ DIS. The contractor shall report to the CSO receipt of NATO SECRET or CONFIDENTIAL information from any source other than through a U.S. Government activity, unless the information is received in connection with approved visits (for example, attendance at a bidders' conference).

91. Subcontracting. Prior to negotiating a NATO classified subcontract in the U.S. or in another NATO country, a U.S. prime contractor shall obtain permission to negotiate such a subcontract from the contracting officer who let the prime contract or his or her designated representative.

Section XII. OVERSEAS OPERATIONS

Part 1. ACCESS TO U.S. CLASSIFIED INFORMATION

92. General.

a. This part sets forth access, safeguarding, and notification requirements for cleared U.S. citizen employees of U.S. contractors assigned to duty stations outside the U.S. These requirements also apply to U.S. citizens who, in addition to being cleared as employees of cleared U.S. contractors, are also dual-status employees of foreign subsidiaries, which are wholly owned and controlled by cleared U.S. facilities.

b. This part does not apply to:

(1) uncleared employees of cleared U.S. contractors who are stationed outside the U.S.;

(2) U.S. citizens who are RFI's or employees of foreign subsidiaries of cleared U.S. facilities, but do not hold dual-status employment with the owning or controlling U.S. facility; and

(3) representatives (not employees) of cleared U.S. contractors.

c. Cleared employees of U.S. contractors stationed overseas are encouraged to attend periodically scheduled security briefings conducted by the OISI. These briefings are designed to familiarize the employees with the international aspects of the DoD Industrial Security Program and the security requirements unique to the foreign countries in which the contractor does business.

d. Whenever a report is submitted to DISCO pursuant to paragraph 6b(9) for a cleared employee assigned overseas, a copy of the report shall be submitted to OISI. * * *

93. Access to Classified Information. Contractors are authorized to grant access to U.S. classified information to their cleared employees who are assigned overseas, subject to the following rules:

a. Access to U.S. classified information identified in this paragraph shall be granted only with the prior written approval of the UA having primary interest if the information concerned is:

(1) TOP SECRET information,

(2) RESTRICTED DATA or FORMERLY RESTRICTED DATA,

(3) COMSEC and SENSITIVE COMPARTMENTED INFORMATION (see CSISM and section IX, ISM),

(4) special access program information (see paragraph 5t), and

(5) information for which foreign dissemination has been prohibited in whole or in part.

b. Access shall be limited strictly to that information required by the employee for performance of the specific duties or contracts for which he or she is assigned overseas. Further, access to U.S. classified information under this section shall be made, to the maximum extent practical, on an oral or visual basis. When physical access is to be granted to an employee, the appropriate safeguarding provisions set forth in paragraph 94 shall be strictly complied with.

c. Access to U.S. classified information for cleared employees assigned overseas may be granted both in the U.S. and overseas.

d. Access to U.S. classified information granted to a cleared employee of a cleared U.S. facility, who is also an employee of a U.S. wholly owned and controlled foreign subsidiary of such a facility, is granted only in his or her capacity as an employee of the cleared U.S. facility. The contractor granting the access is responsible for ensuring that the employee provides adequate safeguards for any classified information disclosed to such employee. In addition, the contractor shall take action, as appropriate, to ensure that U.S. classified information entrusted to the employee is not further released or made available to other employees of the foreign subsidiary.

94. Safeguarding U.S. Classified Information. The following additional safeguards are prescribed in connection with U.S. contractors' overseas operations:

a. Security Classification Guidance. The contractor shall provide security classification guidance, commensurate with the actual performance requirements, to employees performing outside of the U.S. on a classified contract, project, or mission. This guidance may be a DD Form 254, extracts from a DD Form 254, a classification guide, or other guidance as appropriate. If classified documents themselves will provide the necessary guidance, no further guidance is necessary.

b. Transmission. Transmission of classified material to a cleared contractor employee located outside the U.S. shall be strictly in accordance with paragraph 17e. The material shall be addressed to a U.S. military activity or other U.S. Government activity, and shall be marked for the attention of the contractor or the employee for whom it is intended. The U.S. Government activity will notify the contractor or contractor employee of the receipt of the material. Classified material will be transmitted only through U.S. Government channels. Normally, transmission will be by Registered Mail through the U.S. Military Postal Service, or by the DCS. However, the contracting officer may authorize any of the other approved methods of transmission described in paragraph 17e. If disclosure authorization is required and has been obtained, it should be cited in the transmission document with the effective dates and any other limitations. The contractor shall make prior arrangements for the storage of U.S. classified material with a U.S. military installation, the OISI, a military attache, a MAAG, an Office of Defense Cooperation (ODC), or a U.S. diplomatic or consular office prior to transmitting U.S. classified material overseas.

c. Custody and Storage.

(1) Personnel authorized access to U.S. classified material overseas will normally be permitted such access at a U.S. Government activity only. The storage of U.S. classified material overseas at any location other than a U.S. military installation or U.S. Government controlled installation is prohibited.

(2) If in the performance of a contract, project, or mission it is necessary for a contractor employee to physically require temporary custody of U.S. classified material, authorization for removal shall be obtained from the U.S. Government activity. When such custody is authorized, the employee is responsible for personal possession and surveillance of the material at all times. Immediately following the purpose for which the material was needed and the removal was authorized, but in all cases prior to the end of the workday, the material is to be returned to the U.S. Government activity for storage purposes. Movement of the material while in the employee's custody shall be governed by the provisions of paragraph 17h.

d. Disclosure. Except as provided for in paragraph 48, contractor personnel are not authorized to disclose classified information to any foreign government, commercial activity, or entity, or to an international pact organization or its representatives. Cleared contractor personnel overseas may, however, disclose classified information:

(1) to another cleared employee within their company who has been granted an LOC at the required level and who has a need-to-know for access to the information concerned;

(2) to any appropriately cleared military or civilian member of a U.S. UA who has a valid need-to-know; and

(3) outside the contractor's organization within the U.S. only in accordance with this manual, and outside the U.S. only in accordance with instructions from the contracting office of the UA.

95. Overseas Assistance.

a. The DoD has established the OISI to provide administrative assistance for industrial security purposes to U.S. industry in their marketing, liaison, and technical assistance activities outside the U.S. The OISI operates under the supervision and direction of the Deputy Director (Industrial Security), HQ DIS. The OISI acts as a central file for information pertaining to security clearances and security assurances for U.S. contractor employees located outside the U.S. Such information is available for official use by agencies and activities of the U.S. Government, foreign government, NATO, and U.S. contractors. OISI conducts inspections of contractor operations on U.S. installations outside the U.S., when authorized by the Deputy Director (Industrial Security), HQ DIS.

b. The OISI assists U.S. industry by: (i) arranging classified visits for U.S. contractor employees; (ii) providing storage for classified material; (iii) providing mail channels for transmission of classified material between a contractor in the U.S. and an approved destination outside the U.S., when specifically authorized by the Deputy Director (Industrial Security), HQ DIS; (iv) providing security briefings and security certificates, as appropriate; and (v) providing assistance on security matters, such as visits to military activities or contractors outside the U.S.

c. The civilian street address of OISI is: Office of Industrial Security, International, Steenweg Op Leuven 13, 1940 St. Stevens-Woluwe, Brussels, Belgium; the telephone number is 0-322-720-8259. The APO address is: OISI, APO New York 09667-5005. U.S. Government cable address is: OISI, BRUSSELS, BELGIUM; other cables: OISI, American Embassy, Brussels, Belgium. TELEX address is OISI: American Embassy, 21336 Brussels, Belgium. (See appendix VIII for the address of the Mannheim, West Germany Field Office; Yokohama, Japan, Office of Industrial Security, International - Far East and the Seoul, Korea Field Office.) *

96. Notification of Overseas Assignment.

a. Whenever a contractor assigns a cleared employee to an overseas duty station for a period of time over 90 consecutive days, the contractor shall furnish the following information to DISCO on DISCO Form 562:

(1) Full name, social security number, date and place of birth, passport or ID number;

(2) Name and address of the overseas duty station to which the employee has, or will, be assigned;

(3) Notice that the briefing required by paragraph 97 has been accomplished;

(4) The highest level of access to classified information required overseas; and

(5) A detailed justification as to why the employee will require access to classified information overseas in performance of his or her assigned duties, to include identification of the contract or program under which such access is necessary.

b. Subsequent to the overseas assignment of an employee whose PCL has been properly transferred, the contractor shall:

(1) Rejustify to DISCO the employee's continuing need for a security clearance 3 years from the date of initial assignment and every 3 years thereafter; *
*

(2) Advise DISCO of any change in the overseas mailing address or physical address of the affected employee; and

(3) Advise DISCO of the termination of the employee's overseas assignment.

c. Residence or assignment of cleared immigrant aliens outside the U.S. for a period of 90 consecutive days or more in any 12-month period negates the basis on which the LAA was issued, and the LAA will be administratively terminated without prejudice by DISCO on receipt of the contractor notification as outlined in paragraph 6b(6).

97. Security Briefings and Certificates.

a. Cleared employees who are to be assigned to duty stations outside the U.S. are to be briefed on the security aspects of their new positions. These briefings are the responsibility of the contractor. If access to NATO classified information is or may be involved, the briefing shall also cover NATO security requirements as described in section XI.

b. Each cleared employee assigned overseas shall execute and have witnessed a certificate attesting to the following:

(1) The employee has received a security briefing and understands his or her responsibilities.

(2) The employee will safeguard classified information, in accordance with prescribed security standards.

(3) The classified information to which he or she has been granted access will be used only for the purpose for which released.

(4) The employee understands and accepts the fact that his or her LOC may be suspended or revoked for violation of security regulations or improper use of classified information.

(5) The employee understands that he or she may be subject to action under the espionage statutes of the U.S., with respect to the classified information to which access is granted.

(6) The employee also understands that on termination of the purpose for which he or she has been granted access, the employee's responsibilities for safeguarding the classified information continue unabated until the security classification is removed by appropriate government authority. The executed and witnessed briefing certificate shall be retained by the contractor for the duration of the overseas assignment.

c. Subsequent to the initial security briefing, each individual shall be given an annual refresher briefing. A certificate similar to that described above shall be executed annually and maintained as long as the individual is assigned overseas. The certificate shall be modified as necessary to reflect any change in the nature and extent of the classified information to which the individual requires access, and the scope and nature of the threat to which the overseas activity may expose the individual.

d. Normally, refresher briefings should be accomplished on the temporary return of employees to the U.S., or by a security representative of the contractor stationed overseas or on visits overseas. When this is not practical, the briefing and execution of the certificate may be accomplished by OISI at the request of the contractor. Outside of areas serviced by OISI, the contractor may obtain a written briefing statement by mail from the employee.

e. The contractor shall ensure that a company SPP, or supplement thereto, is prepared to cover security procedures at the contractor's overseas locations.

Part 2. ACCESS TO CLASSIFIED INFORMATION OF FOREIGN GOVERNMENTS AND INTERNATIONAL PACT ORGANIZATIONS UNDER A SECURITY ASSURANCE

98. General. In its relations with friendly and allied foreign governments, the U.S. has entered into various treaties and agreements whereby each signatory government agrees to safeguard the classified information released to it by the other government. These range from simple bilateral agreements providing that each government will safeguard, in accordance with mutually agreed procedures, the classified information released to it by the other government, and that the information will not be disclosed to a third country without the consent of the originating government, to multilateral treaties establishing international organizations for concerted defense. Such treaties usually contain either a technical annex establishing the detailed procedures and standards for safeguarding classified information originated or disseminated by the organization, or provisions authorizing the organization to establish mutually agreeable regulations for safeguarding such information.

a. Access to classified information of a foreign government or international pact organization (for example, NATO) is granted by the activity possessing the information, and the scope of access is governed by the regulations of the activity possessing and disclosing the information. Hence, this part prescribes no specific limitations on the access to classified information of foreign governments or international pact organizations, which may be afforded an individual under a security assurance determination. The responsibility for release of the information rests with the foreign activity or international pact organization, or with the contractor, if the information had previously been released to him or her directly by the foreign government, the prime contractor, or an international pact organization without going through government channels.

b. A contractor, or contractor employee, granted access to foreign or international pact organization classified information must take note of the limitations prescribed relative to the further dissemination of such information. For example, NATO classified information cannot be stored in non-NATO countries or released to nationals of non-NATO countries (see paragraph 86), nor can NATO classified subcontracts be let to contractors of non-NATO countries. Foreign countries normally have restrictions on the disclosure and dissemination of their classified information to nationals of a third country.

99. Security Assurance. This paragraph establishes the procedures to assist U.S. cleared contractors in meeting personnel security requirements imposed by friendly and allied foreign governments and international pact organizations with whom the U.S. has entered into either a bilateral or multilateral security agreement for access by U.S. citizens to foreign classified material, which is under the control of the foreign government or organization.

a. The contractor may make application for a security assurance by submitting a written request containing the information required by paragraph (3) below. On application by the U.S. contractor, DISCO will issue a security assurance for currently cleared contractor employees. If the employee does not have a valid LOC, the contractor will submit the following to DISCO:

(1) the forms prescribed in paragraph 26b 1/; or

(2) two copies of DD Form 48-3 1/, if there has been less than a 24-month lapse in a prior employment at which time the employee was granted an LOC; and *

(3) a written request containing the following information:

(a) the title of the position and summary of the duties of the individual for whom the request is made;

(b) the name and location of the overseas office or activity to which the individual is assigned or attached for duty;

(c) the employee's passport or ID card number, if available;

(d) a justification 2/ for the request, which identifies the activity or the subject matter of the proposed visit, sales activity, or contract that will require a security assurance; and

---

1/ Under Item 11 of DD Form 48 or 49, or Part II, item 8a of DD Form 48-3, the applicant shall list both his or her overseas residence and permanent U.S. residence, if one is maintained. In addition, under Item 12 of DD Form 48-3, the applicant shall list all previous overseas residences. Under Item 13c of DD Form 48, Item 13c of DD Form 49, or Item 11 of DD Form 48-3, the applicant shall show the names and addresses of all firms or foreign government activities with which the applicant is associated, the relationships and duties in connection therewith, and the nationality of the controlling interests of the firms involved.

2/ The need and justification may be stated in general terms. For example: "In order to participate in the negotiation of contracts with foreign governments or international pact organizations, it will be necessary for him or her to have access to classified information of those countries and organizations (identify countries and/or organizations)," or, "As our overseas electronics engineer, it will be necessary for him or her to have access to foreign classified information in order to service equipment sold by our company to (identify country or countries concerned)."

(e) a statement providing the name and address of the foreign government activity or international pact organization, requesting the U.S. security assurance and the level of access required. If access to U.S. originated, and appropriately marked, classified information will be granted to the employee by the foreign requester, the contractor will execute and maintain one copy of the briefing certificate prescribed by paragraph 97.

(4) In the case of persons who are employees of foreign subsidiaries, the application shall be sent through the parent organization or the PMF.

(5) On termination of employment or termination of assignment overseas, the security assurance determination is void and the contractor shall immediately notify DISCO of the individual's changed status by means of DISCO Form 562.

(6) Requests for reinstatement of a security assurance determination will be processed in the same manner as an original request.

(7) If an individual, on whom a security assurance has been given, is subsequently employed by a cleared contractor and requires a U.S. security clearance, the contractor may make application within 24 months for a * security clearance for the individual under section III by submission of a DD Form 48-3 (see paragraph 26d). If the time lapse is more than 24 months, the forms prescribed by paragraph 26b shall be submitted.

b. Normally, requests for a security assurance determination will be limited by the foreign government or international pact organization to CONFIDENTIAL or SECRET access. In exceptional cases, a request for a TOP SECRET security assurance, received from a foreign government or international pact organization, will signify that access to TOP SECRET information is necessary for the consummation of a specific contract, project, or activity. TOP SECRET security assurance determinations shall be limited to the specific contract, project, or activity for which they are granted.

Section XIII. SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS

Part 1. GENERAL

100. Reserved.

101. Applicability.

a. This section establishes special security measures for the safeguarding of classified information and material processed by or in automated information systems (AIS) in the custody and control of contractors, including organizations that provide contractual computing services to UA's or their contractors. Classified information processed by or contained in an AIS shall be safeguarded by the employment of collective security measures, controls and constraints which will provide an acceptable level of protection.

b. Security measures for AIS's located on UA installations, that are operated by the contractor, are prescribed by the controlling UA. However, the Commander or Head of the installation may elect to declare the contractor activity a facility and request the CSO to assume security cognizance, in which case the provisions of this section will be applicable.

c. Security measures for computers which are embedded as an integral element of a larger system to perform or control a function, such as in test stands, simulators, control systems or weapons systems, should be established concurrently with the design and development of the system, using the fundamental security concepts outlined in this section. If the security requirements for such systems are not provided with the contract, contractors should request them from contracting officers. In the absence of such requirements from contracting officers, the security requirements and procedures of this section will be applied to the extent appropriate to the situation, as determined by the CSO.

d. This section prescribes the requirements for the protection of information classified in one of the three classification levels, namely: TOP SECRET, SECRET or CONFIDENTIAL. Special access programs may impose additional security requirements, or limitations, for specified types of classified information which are beyond the requirements prescribed herein. Contractors shall implement special access program requirements when included in a DD Form 254, or other appropriate contract-related document.

102. Objectives.

a. The collective security measures and controls employed must ensure that an AIS which handles classified information will, with reasonable dependability, prevent: (i) unauthorized access to classified information during, or resulting from, the processing of such information, and (ii) unauthorized manipulation of the AIS which could result in the compromise of classified information.

b. To accomplish the foregoing, collective security controls shall, to the maximum extent possible, provide the following:

(1) Individual Accountability. The identity of each user of the AIS shall be positively established, with access to the system and to information contained in the system controlled and open to scrutiny.

(2) Physical Control. The AIS shall be externally protected to minimize the likelihood of: (i) unauthorized access to system entry points and to classified information in the system, and (ii) unauthorized modification of the computer hardware.

(3) System Stability. All elements and components of the AIS shall function in a cohesive, identifiable, predictable and reliable manner such that malfunctions can be detected and reported to maximize security control.

(4) Data Continuity. Each file or collection of classified information in the AIS shall have an identifiable origin and use. Access to maintenance, movement and disposition of classified information shall be governed on the basis of security classification, PCL and need-to-know.

(5) Least Privilege. The AIS shall function to provide each user access to all of the information to which entitled, but no more.

(6) Communications Security. Communications lines and links shall be secured in a manner appropriate for the classified information being transmitted through the lines and links.

(7) Classified Information Control. Classified information handled and produced by the AIS, and stored in or on recording media, shall be safeguarded as appropriate for the classification level of the information.

Part 2. REQUIREMENTS

103. General.

a. AIS security shall consist of the employment of appropriate administrative, procedural, physical, personnel and communications security measures and controls, along with protective features in the system's hardware and software. The procedures and methods necessary to safeguard classified information depend on the nature of the AIS, the uses to which it is put, and the mode of operation as set forth in paragraph 104. It is the contractor's responsibility to safeguard all classified information processed by or contained in an AIS and ensure that approved security controls are in place and are effective.

b. Approval, in writing, of the CSO is required prior to processing any classified information in an AIS. To obtain approval, the contractor shall prepare an SPP describing the AIS and the security controls implemented for that AIS in accordance with paragraph 112d. The SPP will provide the basis from which the CSO will approve and inspect the AIS for the proper safeguarding of classified information. If changes are made to the AIS subsequent to approval, or to approved security measures and controls, reapproval by the CSO may be required prior to processing classified information. Reapprovals are required because of: (i) major changes in personnel access requirements, (ii) relocation or structural modification of the computer facility or remote terminal areas, (iii) additions, deletions or changes to computer hardware that impact approved security controls, (iv) software changes that impact security protection features, and (v) changes in clearance, declassification, audit trail or hardware/software maintenance procedures.

c. The contractor shall appoint an employee as the system security officer (SSO) for each facility with an AIS approved for the processing of classified information. The SSO, where different from the FSO, shall be responsible to the FSO for implementation of procedures and practices prescribed for the safeguarding and control of the AIS and for the processing of classified information. Where there are multiple AIS's in a facility, or multiple shifts of classified operation, and the contractor deems that the SSO cannot effectively discharge that responsibility, then one or more system security custodians, working under the guidance of the SSO, may be designated to accomplish security responsibilities for the separate systems or different shifts.

d. The establishment and maintenance of hardware and software integrity is essential to ensuring continued safeguarding of classified information in an approved AIS. Integrity of the hardware is attained through the provisions of paragraph 106. All software and data used during classified processing periods must be safeguarded and handled as prescribed in paragraph 108.1.

104. AIS Security Modes of Operation. System security modes are authorized variations in security environments and methods of operating AIS's that handle classified information. The modes are primarily defined by the manner in which basic access requirements for user PCL and need-to-know are implemented for the AIS. The modes involve a varying mix of automated (that is, hardware/software) and conventional (that is, personnel, physical, administrative, procedural and, where appropriate, communications) security measures and techniques in discharging these basic access requirements. In all modes, the total integrated set of automated and conventional security measures applied to the AIS shall be based on the objectives set forth in paragraph 102. A contractor may accordingly process, store, use and produce classified information in an AIS that is operating in one of the following modes:

a. Dedicated Security Mode -- All users with access to the AIS must have both a PCL and the need-to-know for all information then contained in the system.

(1) The objectives of paragraph 102 are normally fulfilled by the collective security controls established for: (i) the computer facility, (ii) all peripheral devices and input/output terminals, (iii) areas containing remote devices and terminals connected to the system, and (iv) the interconnecting communication lines and links.

(2) These controls shall conform to those required for the protection of the highest classification level and most restrictive type of information then contained in the system.

b. System High Security Mode -- All users with access to the AIS must have a PCL, but not necessarily the need-to-know, for all information then contained in the system.

(1) The objectives of paragraph 102 are normally fulfilled by application of the controls enumerated in paragraph a(1) above. The process of identifying, separating and controlling users and classified material on the basis of PCL and need-to-know, and classification level, respectively, shall be provided by operationally acceptable controls that include passwords, add-on software packages and identification devices such as fingerprint, hand or retinal scanners, and voice or signature comparison devices. A trusted computer system listed on the EPL [1] with an evaluation rating of at least C2 is considered to provide an acceptable level of control for this mode of operation.

(2) Controls shall conform to those required for the protection of the highest classification level and most restrictive type of information then being handled by the system.

c. Multilevel Security Mode -- Some users with access to the AIS do not have a PCL for all classified information then contained in the system. This mode of operation provides a limited capability for concurrent processing by users with different PCL's and need-to-know in a system that may contain more than one level of classified information. Concurrent access to the AIS is restricted to users with two adjacent PCL levels, that is, CONFIDENTIAL and SECRET, or SECRET and TOP SECRET.

(1) The objectives of paragraph 102 are normally fulfilled by application of the controls enumerated in paragraphs a(1) and b(1) above, with the exception that for this mode of operation, a trusted computer system listed on the EPL [1] must have an evaluation rating of at least B1 if the system contains SECRET information; and at least B2 if the system

---

[1] The EPL (Evaluated Products List for Trusted Computer Systems) is published in conjunction with the National Computer Security Center's commercial product evaluation program - in which commercially available systems are formally evaluated against the DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) and assigned an overall class rating based on the system's ability to meet the requirements of the Criteria. The EPL and DoD 5200.28-STD are available at the CSO and from the DoD Computer Security Center, 9800 Savage Road, Fort George G. Meade, Maryland 20755.

contains TOP SECRET information. In addition, the multilevel security mode requires fulfillment of the requirements of paragraph 104.1 for the concurrent processing of multiple levels of classified information.

(2) Controls for the computer facility shall conform to those required for the highest classification level and most restrictive type of information then being handled by the system. Controls for remote terminal areas shall conform to those required for the highest classification level and most restrictive type of information accessed through the terminal under system constraints, including unclassified.

(3) A request for approval to operate an AIS in multilevel security mode shall clearly explain why this mode of operation is required at the contractor facility. The SPP describing the AIS and its security measures should be as complete as possible and specifically enumerate the augmenting measures that remove or substantially reduce system software and/or hardware vulnerabilities and associated risks. Methods and techniques that may be used to augment or enhance the AIS security include:

(a) the employment of hardware, software and/or firmware, alterable only at the computer facility, for critical AIS security functions such as identification and authentication of individual users, separation of users and data, data labeling, identification and segregation of output and labeling of all human-readable output;

(b) the employment of system architectures, stringent configuration management controls, and facility management procedures that assure: (i) separation of files and processes, (ii) access limitations to physical devices, and (iii) trusted recovery in the event of system failure or malfunction;

(c) audit trails of identification/authentication events, individual user actions, accesses to data, and other security-relevant events that signal potential violations of security policy;

(d) interconnection of remote terminals via one-way information communication links, wherein substantive information can be transmitted only in one direction. (Circuits that require two-way communication for specific control functions in order to properly receive substantive information may be considered one-way circuits when it is determined that only control information can be transmitted in both directions);

(e) assignment of terminal security officers with a PCL for the highest classification level of the approved AIS in remote terminal areas;

(f) system splitting via hardware/software that is alterable only at the computer facility; and

(g) limitations on user capabilities, such as restriction to fixed-query access only, and prohibition of assembler and machine language programming.

104.1 Concurrent Processing of Multiple Classification Levels. The concurrent processing and storage of more than one level of classified information, together with unclassified information, is authorized in any of the foregoing system security modes. All information output from, or stored in, the AIS must be handled as the highest classification level of information being processed until reviewed, correctly identified and segregated by properly cleared and responsible personnel. The process of identifying, segregating and marking the different levels of information may be by automated means provided that: (i) the AIS is a trusted computer system listed on the EPL 1/ with an evaluation rating of at least B1, or (ii) the following minimum conditions are met:

a. The contractor and the CSO have determined that the design and operation of the AIS will, with reasonable dependability, automatically provide for consistent and correct identification and segregation of: (i) information of different security classification levels, (ii) certain additionally restrictive types of classified information, when such concurrent processing is authorized by special access program directives, and (iii) unclassified information.

b. Measures have been implemented to monitor the AIS for malfunctions and occurrences that may adversely affect the dependability of such automated identification and segregation.

c. Procedures have been instituted which will, in the event of such malfunction or occurrence, control all system output as the highest classification level and most restrictive type of information in the system, pending a determination of actual classification levels. These procedures shall remain in effect until the cause of the malfunction is determined and corrected.

d. All users of the system have been advised that this automated identification and segregation option has been implemented and have been instructed to return to the SSO any system output that has an incorrectly labeled classification level or was not requested by that user. A determination shall be made of the cause of the incorrect system action. A record of each instance, and the corrective action taken, shall be maintained for at least one Government inspection cycle.

105. Personnel Security. As provided below, access to an AIS processing classified information shall be limited to authorized persons who have a PCL and need-to-know for the highest classification level and most restrictive type of information they will access under system constraints.

a. System Users. Users are authorized persons with the ability and means to approach, communicate with (input to or receive output from) or otherwise make use of any information or component in the AIS. Personnel who code, test or maintain application programs used to produce a service or product are considered to be users. Those authorized persons who make use of application programs via over-the-counter or remote means, and who have the ability and means to create, destroy, change or retrieve data or program instructions in the system, are also considered to be users. All users shall have a PCL and need-to-know as required for the security mode of operation (paragraph 104). The following personnel are not considered to be users:

(1) Personnel who only receive computer output products from the AIS and do not input to or otherwise interact with the system (that is, no "hands on" or other direct input or inquiry capability) are not considered to be users. Accordingly, they are not subject to the PCL requirements of this section. Such output products, however, shall either be reviewed by appropriately cleared and responsible personnel prior to dissemination, or otherwise determined to be properly identified and segregated as to content and classification, as prescribed in paragraph 104.1.

(2) Personnel who produce application programs and changes thereto, or prepare data that may be input to the AIS during classified processing periods, may be excepted from PCL requirements provided they do not receive unreviewed output products from the AIS, or otherwise directly interact with the AIS during classified processing. Such software or data must be introduced into the system as prescribed in paragraphs 108.1c(4) and d, respectively.

b. System Support Personnel. Personnel who administer and operate the AIS are considered to be system support personnel. They shall have a PCL for the highest classification level and most restrictive type of information the AIS is approved to process. This category includes all persons in the immediate vicinity of the system attending to the operation, control and functioning of the system, as well as those persons who design, program, modify, test or install system software used during classified processing periods. Access to specific classified material shall be governed by need-to-know in relation to individual duties and responsibilities.

c. Maintenance Personnel. All persons involved in hardware maintenance or repairs requiring entry to the computer facility, or access to any parts or components of the AIS, where: (i) the complexity of the AIS, (ii) the nature of maintenance/repairs to be performed, (iii) the frequency of visits, (iv) the amount and classification level of information processed, or (v) the availability of knowledgeable escorts makes escorting impractical, shall have a PCL at least to the classification level for which the AIS is approved to process. Maintenance personnel who do not have the appropriate clearance must be accompanied by an escort duly designated by the SSO. Escorts must be cleared at least to the classification level of the system approval, and take all reasonable measures to control the activities of the individual being escorted so that the integrity of the AIS is maintained.

d. Visitors. Persons visiting the area on a one-time or infrequent basis, and who will not have access to classified information or to the system hardware or software, may be admitted to the area when accompanied by a duly designated escort who will control visitor access and be responsible for visitor activities while in the area. For other persons requiring entry into the computer facility or remote terminal areas who will have access to classified information or to the computer hardware or software, the visitor control procedures of the ISM are applicable.

e. Security Training and Awareness. It is the responsibility of the SSO to indoctrinate all system users and support personnel in: (i) the need for sound security practices in protecting information handled by the AIS, including all output products, (ii) the specific security requirements associated with the AIS in terms of system security mode of operation and user access requirements, (iii) the security reporting procedures in the event of system malfunctions or security incidents, and (iv) what constitutes unauthorized actions with regard to system utilization. System users shall be indoctrinated prior to being granted system access, and reindoctrinated on a recurring basis. System support personnel shall also be indoctrinated in appropriate operational security procedures for the particular AIS and facility before they assume their duties. Additional briefing specifics for AIS's approved to concurrently process multiple levels of classified information are identified in paragraph 104.1.

106. Physical Security.

a. Physical security safeguards and access controls must be established and continuously maintained for AIS's approved for the processing of classified information.

b. When the AIS is used for classified processing, physical security safeguards and access controls for the computer facility, areas housing remote terminals connected to the system, and the communications lines and links shall conform to those required for the highest classification level and most restrictive type of information being processed.

(1) Where two or more AIS's are located in the same area, and the equipment comprising each AIS is located and controlled so that direct physical access is effectively limited to that system, the area limited to each system may be considered that system's "computer facility." The measures and techniques for so "isolating" that system shall be reflected in the SPP.

(2) Remote terminals not used during classified processing periods shall be disconnected at the computer facility by: (i) physically disconnecting the device, (ii) use of channel or transmission line hardware switches, or (iii) use of software disconnect routines. Software disconnect routines may be used only for AIS's which handle information classified no higher than SECRET. Such routines must be documented to clearly indicate physical actions and logic processes used, and be verified in writing by the contractor at least every 90 days to ensure continued effectiveness. These provisions are not applicable to specifically designated remote terminals connected to systems approved to operate in the multilevel security mode (paragraph 104c(3)(d)).

c. When the AIS is used to process classified information unattended, or when classified information is left in the system or elsewhere unsecured within the computer facility or remote terminal areas, closed areas in full compliance with paragraph 34, ISM, must be established. Computer hardware and associated media may also be stored in cabinets, strongrooms and vaults as specified in paragraph 14, ISM.

d. During unclassified processing periods, controls must be maintained to prevent unauthorized modification of the computer hardware. Continuous physical protection can be attained through one or a combination of the provisions of paragraphs e(1)-(4) below.

e. When the AIS is not in use, and all classified information has been removed from the system and properly secured, continuous physical protection to prevent or detect unauthorized modification of the computer hardware can be attained through one or a combination of the following:

(1) Closed areas, in full compliance with paragraph 34, ISM, may be established for the computer facility and remote terminal areas. Supplemental controls (that is, patrol or intrusion detection systems) are not required for closed areas used solely for the physical protection of computer hardware.

(2) Computer hardware and associated media may be stored in approved cabinets, strongrooms and vaults in accordance with paragraph 14, ISM. Supplemental controls are not required for approved containers used solely for the physical protection of computer hardware.

(3) Continuous supervision may be maintained by cleared and specifically designated personnel who are in a physical position to exercise direct security controls over the AIS (for example, guard station or closed circuit TV monitor). Use of supplemental or supplanting IDS is authorized in accordance with the provisions of paragraph 35, ISM.

(4) This last alternative is not authorized for the protection of AIS's approved to process TOP SECRET information. Protected areas can be established and maintained for the computer facility and areas housing remote terminals. A protected area is continuously protected by a collective level of physical security safeguards and personnel access controls keyed to the prevention or detection of unauthorized modification of the computer hardware. The specific security measures established by the contractor will vary depending on: (i) the overall physical security controls already in effect at the facility, (ii) the environment in which the AIS is employed, the relative potential for unauthorized access, and the effectiveness of safeguards in reducing the risks of identified threats, (iii) the classification level and volume of the information to be processed, and (iv) the consistency, reliability, and auditability of the safeguards to be employed. Appropriate physical safeguards may include: (i) locks on doors to buildings and rooms which provide reasonable protection against surreptitious entry into the area, (ii) authorized guards or employees stationed so as to control entry into the immediate area housing the computer hardware, (iii) IDS, and (iv) the use of equipment covers, enclosures, seals

or locks to prevent or detect unauthorized access to the inside of the equipment. When surreptitious entry and/or modification of system hardware is suspected, a thorough inspection of the protected area and equipment must be conducted by the SSO (or designee) prior to classified processing. Such incidents must be recorded in the audit trail system.

107. Reserved.

108. Reserved.

108.1 Protection of Software and Data.

a. System Software. When system software used during classified processing periods is not in the system, it must be safeguarded commensurate with the requirements for the highest level of classified information processed. System software may be retained in the AIS on nonremovable storage media when the AIS is not in use, provided that continuous physical protection of the hardware (and the system software) is maintained as set forth in paragraph 106e. System software, whether obtained from sources outside the facility or developed by the contractor, shall be safeguarded from the earliest feasible time that it is in the custody and control of the contractor and is identified for use during classified processing periods. System software and modifications thereto shall be developed by contractor personnel who meet the PCL requirements of paragraph 105b.

b. Classified Application Software. Application software which in itself contains classified data or comments, or implements classified processes or algorithms (as specified in the contract), shall be produced, marked and protected as any other classified material in compliance with the provisions of the ISM. These provisions are applicable to both human and machine readable versions of the software, as well as to supporting and related documentation. Changes to classified software shall be made only by appropriately cleared contractor personnel.

c. Unclassified (or Lower Classified) Application Software.

(1) Unclassified application software to be used during classified processing periods: (i) may be produced as an end item for delivery to the UA, (ii) may be produced for use in a classified end item or weapon system during performance of the contract, (iii) may be developed incidental to the performance of the contract, (iv) may have been developed previously by contractor personnel for other purposes or another contract, or (v) may be obtained from sources outside the facility.

(2) When application software is contractually produced for delivery as an end item, or for use in a classified end item or weapon system, the contract should specify whether it is classified or unclassified. If the security requirements for contractual software are not provided with the contract, contractors should request them from contracting officers. In the absence of such requirements from contracting officers, the requirements and procedures of this section will be applied as appropriate.

(3) Application software that will be used during classified processing periods shall normally be produced and maintained by appropriately cleared personnel (paragraph 105a) under accepted software configuration management controls that provide reasonable assurance that the integrity of the software will be maintained throughout its development and operational life-cycle. Such software must be safeguarded commensurate with the requirements for the highest level of classified processing with which it will be used. The primary objective is to prevent unauthorized access to classified information during, or resulting from, the processing of such information because of malicious logic introduced into the application software. Unauthorized disclosure of classified information can also be prevented by ensuring that uncleared (or lower cleared) application programmers do not receive unreviewed output products from classified processing periods or otherwise interact directly with the system during classified processing (paragraph 105a(2)). It should be noted that the prevention of unauthorized destruction or modification of classified information is not expressly provided for in this section.

(4) It is recognized that application software may have been produced for other purposes by contractor personnel without the requisite PCL or obtained from other unprotected sources. Before such software can be used in classified processing periods, it must be reviewed, approved and authorized for use by appropriately cleared and knowledgeable contractor personnel who understand the security implications of the software being reviewed. The software must then be introduced into the system in a read-only or write-protected manner during the classified processing period. This is to prevent possible unauthorized disclosure of classified information by precluding the ability to write (intentionally or accidently) classified information to media associated with the unclassified (or lower classified) software. The software should be copied to dedicated and previously protected media for use during subsequent classified processing periods, or it may be executed during the classified processing period in which loaded. Subsequent changes to the safeguarded software must be authorized, made by appropriately cleared personnel, fully tested and implemented in a controlled manner.

(5) Unclassified application software used during classified processing periods may be retained in the AIS on nonremovable storage media when the AIS is not in use, provided that continuous physical protection of the hardware (and the application software) is maintained as set forth in paragraph 106e.

d. Data. During classified processing periods, unclassified (or lower classified) input data shall be introduced into the system in a read-only or write-protected manner. Unclassified data may be retained in the AIS on nonremovable storage media when the AIS is not in use provided that continuous physical protection of the hardware (and the data) is maintained as set forth in paragraph 106e.

e. Media Control. Protection requirements for storage media on which classified software and data reside will be attained by marking, recording (that is, an accountability record) and storing the media in accordance with provisions of this manual. Safeguarding controls shall be commensurate with the requirements for the highest classification level of * * * * * software or data contained thereon, and shall be maintained until the media are declassified pursuant to paragraph 116. Safeguarding controls for media which have been cleared according to the provisions of paragraph 115 can be obtained by the continuous physical security requirements of paragraph 106e. * * * * * *

109. Transmission Controls.

a. Transmission and communication lines and links between the components of an AIS (for example, the computer facility and remote terminals) may be used to transmit classified information as follows.

b. Inter-Complex. Transmission of classified information between contractor facility complexes must be over approved CRYPTOGRAPHIC communication circuits, and only with the prior written approval, and in accordance with the instructions, of the contracting officer.

c. Intra-Complex. Transmission within a contractor's complex may be over approved CRYPTOGRAPHIC communication circuits or over wire or fiber optic circuits. Such circuits shall be protected by an in-depth physical security system to include the following:

(1) Dedicated Lines. Transmission lines must be dedicated to the computer and the remote terminals which are approved for the handling of classified information. Transmission lines shall be separated from, and not included in, cables that contain other lines not dedicated to the transmission of classified data, nor be connected to, or go through, telephone frames, switching equipment or any other telephone equipment.

(2) Line Protection. In the event transmission lines cannot be contained entirely within areas secured for the highest level of classified information transmitted, continual protection/surveillance of the lines shall be accomplished by: (i) alarming the transmission lines and conducting periodic checks of the lines and alarm integrity, (ii) constant surveillance of the lines by appropriately cleared and designated personnel, or (iii) a combination of physical protection of the transmission lines in conjunction with periodic inspections or guard patrols. Specific criteria for the physical protection, alarming and surveillance of transmission lines will be provided by the CSO.

110. Subcontracting Controls.

a. A contractor may subcontract to use the approved AIS of another contractor for the processing of classified material. Approval by the CSO(s) will be based on the security measures and procedures described in the SPP of both the using contractor and the subcontractor providing the AIS (that is, the lessor).

(1) The lessor is responsible for ensuring that the integrity of the AIS is maintained at all times in accordance with the provisions of this section. Audit trail records shall identify classified processing periods of the using contractor(s) and the level of classified processing.

(2) The using contractor shall maintain adequate administrative, procedural, physical and personnel security controls during classified processing periods and assure that residual classified information is not retained in the AIS when physical control is relinquished back to the lessor. If a representative of the lessor remains in the computer facility for equipment maintenance or other purposes during the classified processing period, the lessor is responsible for ensuring that the representative has the appropriate PCL. All classified information and material belonging to the using contractor, including processing audit trails, shall be removed from the lessor's premises at the end of the classified processing period.

b. A contractor may have a subcontractor process classified material provided that the subcontractor's AIS has been approved pursuant to this section. The subcontractor shall maintain audit trails of all classified processing and ensure that the integrity and separation of classified material is maintained at all times.

111. Audit Trails.

a. Audit trails provide a chronological record of the use of the AIS and system support activities related to classified processing. Approved audit trails will provide detailed records of system activities to facilitate reconstruction, review and examination of events surrounding or leading to possible compromise should a security malfunction occur. The audit trail system must record significant events occurring in the following areas of concern: (i) interactivity between users of the system and system support personnel who operate the system (for example, preparation of input data and dissemination of output products), (ii) activity within the AIS environment (for example, modification of operational security-related controls), and (iii) internal computer activity (for example, user accesses to the system and classified files).

b. Audit trail records may be manual, automated or a combination of both, and may be stylized to the particular facility, AIS and security mode of operation. Systems approved to process classified information should utilize most, if not all, of the audit trail records and logs listed below. The contractor's SPP must identify and describe those audit trails that are applicable to the particular system and mode of operation:

(1) Personnel access to the computer facility and remote terminal areas.

(2) Start and stop of classified processing periods.

(3) Initiation and termination of pertinent system security-related events (for example, upgrading and downgrading actions, disconnecting and reconnecting remote terminals/devices, and application/reapplication of seals to equipment/device covers).

(4) Actions to open, close, create and destroy classified files.

(5) System aborts and anomalies during classified processing periods (to include time of the incident, identification of users, programs and classified files involved, and corrective actions taken).

(6) Maintenance and repair of computer hardware (to include adding, changing and removing equipment and devices). Systems and equipment sent outside the facility for maintenance or repair shall be declassified in accordance with paragraph 116.

(7) Functions initiated by console operators during classified processing periods.

(8) Logon and logoff of users during classified processing periods.

(9) Attempts to access programs or classified files by unauthorized users.

(10) Generation, modification and implementation of system and application software used during classified processing periods.

c. The SSO or custodian shall review the audit trail logs at least weekly to ensure that all pertinent activity is properly recorded and that appropriate action has been taken to correct any anomalies. Records of the weekly reviews must be maintained and retained by the reviewer(s).

d. Audit trails in accord with the above may not be applicable to computers embedded in test stands, simulators, control systems or weapons systems. Such systems may require individualized consideration by the CSO.

e. Audit trail records shall be retained for at least 6 months and through one Government inspection cycle.

Part 3. PROCEDURES

112. AIS Security Approval.

a. The approval (or reapproval) of an AIS to process classified information commences when a formal written request, accompanied by an SPP describing the AIS and its security measures, is received at the CSO. The SPP may be an addendum or supplement to the facility SPP. The SPP submitted by the contractor will be safeguarded and available only to authorized Government personnel.

b. System Reapproval. A request for reapproval of an AIS shall be submitted as required in paragraph 103b. Revisions to the SPP reflecting changes in the AIS and/or its security measures and controls must accompany the request.

c. Withdrawal of Approval. If the security measures and controls established and approved for an AIS do not remain in place and effective, approval of the AIS can be withdrawn by the CSO. Approval may also be withdrawn if the AIS has not processed classified data during the previous 9 months, provided no valid requirement exists for the AIS to remain approved.

d. Standard Practice Procedure. The contractor shall prepare and maintain an SPP to provide the basis for the CSO to approve and inspect the AIS. Therefore, the SPP must contain complete and accurate descriptive information about the AIS, its classified usage, and the security controls and procedures to be implemented for that AIS. Where similar systems are located within the contractor's facility, a single SPP covering the repetitive features, safeguards and controls of all the systems is permissible. Addendums to this SPP will be used to identify the location of each AIS, as well as any nonstandard features or procedures associated with a particular system. The following specific areas shall be addressed in the SPP.

(1) Identification. Identify the AIS used for classified processing, its physical location, the AIS security mode of operation, the level of classified information to be processed, and the SSO and custodian(s), if any.

(2) Summary of System Usage. Describe the classified use or purpose of the AIS, indicating local and remote capabilities, hours of operation, when classified processing will occur, and percentage of utilization for classified processing. In the case of multiprocessing systems, indicate the mixture of programs/applications during classified processing. Also describe storage media and input/output devices used during classified processing and the highest classification level of information on, or processed through, each.

(3) Hardware. List and describe all equipment comprising the AIS, including the size and type of internal memory and other storage media. Include diagrams, schematics and/or floor plans as appropriate. Describe disconnect methods and switching devices for disabling equipments not to be used during classified processing periods.

(4) Software. Identify system software used during classified processing, how maintained and how safeguarded. Describe security/protective features available in system software and/or coded into application programs, how they are used during classified processing, and the means to ensure that they are functioning effectively. (See paragraph 108.1.)

(5) Teleprocessing. Identify all teleprocessing equipments and transmission lines employed with the AIS and indicate methods of disconnecting those not used during classified processing. Describe teleprocessing configurations and interfaces during classified processing, general usage of remote devices, protection procedures for transmitted data, and physical controls to protect transmission lines. (See paragraph 109.)

(6) Personnel. Describe the security responsibilities of personnel, controls to restrict personnel access to the computer facility and remote terminal areas during working and non-working hours, security indoctrination of personnel, and control of visitors and maintenance personnel. (See paragraph 105.)

(7) Physical. Describe physical characteristics and safeguards to control access to the computer facility and remote terminal areas during working and non-working hours. (See paragraph 106.)

(8) General Access Controls. Describe controls which restrict access into the AIS and to classified information in the AIS during classified processing periods (such as passwords, isolation of users, sign-on/sign-off procedures and terminal identification techniques). For example, if passwords are used, describe the issuance, length, control and protection of the passwords, frequency of changing passwords, how passwords are used and their access privileges, and detection and reporting of unauthorized access attempts. Passwords should be: (i) at least six alphanumeric characters, (ii) classified the same as the highest classification level of information for which the user is authorized to access in the AIS, and (iii) changed at least every 3 months, on termination of employment or reassignment of any user possessing knowledge of the password, or when the password is believed to have been compromised or subjected to compromise.

(9) Operating Procedures. Describe start-up procedures for classified processing (such as clearing the area, physical safeguards, disconnections and loading the system), procedures during classified processing (such as handling of input/output, audit trails and emergency procedures), and procedures for shut-down of classified processing (such as clearing or declassifying storage, removal of classified media, unloading the system and reconnections).

(10) General Storage, Protection and Control. Describe the control, handling, marking, storage and accountability of classified materials such as software, input data, output products and storage media, and procedures for the clearance, declassification and destruction of storage media containing classified information.

(11) Audit Trails. List, describe and provide exhibits of all automatic and manual audit trail records which provide a documented history of the use of the AIS for classified processing. (See paragraph 111.)

(12) Subcontracting. Identify cleared subcontractor(s) used to process classified information. Describe the arrangements and procedures for the classified processing. (See paragraph 110.)

(13) Emergency Plan. Describe additional procedures not covered above to be employed in case of security violations, system crashes or other emergencies during classified processing (such as personnel to notify, protection of hardware and classified material, and control of uncleared emergency personnel).

113. AIS Security Level Upgrading. To adjust the AIS to a higher security level for: (i) initiating a classified processing period after the AIS has not been in use, (ii) changing from an unclassified to a classified processing period, or (iii) processing a higher level or more restrictive type of classified information, the following procedures shall be implemented:

a. If the AIS has not been in use or has been processing unclassified information unattended, and continuous physical protection has been provided in accordance with the provisions of paragraph 106e(4), the immediate area shall be inspected for signs of unauthorized entry and/or the equipment shall be inspected for signs of unauthorized access to the interior (for example, loose covers, broken seals, missing screws, pry marks or scratches). If signs are found that unauthorized persons may have gained entry into the area or access inside the equipment, the SSO shall be notified immediately. Before using the AIS for classified processing, the computer hardware shall be inspected and/or tested to reveal any hardware modifications. Appropriate software diagnostic routines may be used in this process.

b. All remote terminals that are not secured to the higher level of classified processing to be accomplished shall be disconnected in accordance with the provisions of paragraph 106b(2).

c. All storage media of a lower classification level shall be disabled, disconnected or dismounted, and either removed from the area or otherwise segregated within the area.

d. All internal memory, buffer storage and other reusable storage devices not disabled, disconnected or dismounted shall be appropriately cleared, as set forth in paragraph 115.

e. Higher level security controls for the computer facility and connected remote terminal areas, including the implementation of access controls, personnel clearance and physical security requirements, shall be imposed.

f. A dedicated and previously protected copy of the system software shall be loaded into the AIS. However, if the system software has been retained in the AIS on nonremovable storage media in consonance with paragraph 108.1a, the system software need not be reloaded if: (i) the AIS has not been used since the last classified processing period, (ii) the security level of the last processing period was not lower than the security level of the processing period being established, (iii) continuous physical protection of the AIS has been maintained in accordance with the provisions of paragraph 106e, and (iv) there are no signs of unauthorized entry into the area and/or access to the AIS.

g. Lower classified or unclassified application software and data shall be loaded into the AIS in accordance with the provisions of paragraph 108.1c(4) and d, respectively. However, if unclassified application software or data was retained in the AIS on nonremovable storage media in consonance with paragraph 108.1c(5) and d, respectively, the application software or data need not be reloaded under the same conditions as specified in paragraph g above for system software.

h. A final security check shall be made of the foregoing prior to initiation of the higher level processing. Audit trail records will be maintained indicating what actions were taken, when and by whom.

114. AIS Security Level Downgrading. To adjust the AIS to a lower security level for: (i) processing a lower level or less restrictive type of classified information, (ii) changing from a classified to an unclassified processing period, or (iii) establishing a level of continuous physical protection when the AIS is not to be used (in accordance with the provisions of paragraph 106e), the following procedures shall be implemented:

a. All removable storage media (including that containing the safeguarded higher level software), listings, ribbons, cards, classified waste and so on, associated with the higher level of classified processing, shall be dismounted, collected, marked, removed and appropriately secured. Where area controls for the computer facility or remote terminal areas are continuously maintained at the higher classification level, the removable storage media may be segregated within, rather than removed from, the area, provided the higher level classified information is not online or otherwise accessible through the AIS.

b. All internal memory, buffer storage and other reusable storage devices remaining on the AIS shall be cleared in accordance with the procedures in paragraph 115.

c. A security check shall be made of the foregoing and audit trail records maintained indicating what actions were taken, when and by whom.

115. Media and Equipment Clearance.

a. To preclude unauthorized disclosure of classified information when either upgrading or downgrading the security level of the AIS, all internal memory, buffer storage and other reusable storage devices used during the prior processing period must be cleared before reutilization of the AIS. The CSO will advise the contractor of authorized procedures for clearing and verifying specific memories, storage media, devices and equipment.

b. Internal Memory. Internal memory, registers, buffers and circuitry of most systems and devices can be cleared by overwriting each memory position at least once with unclassified information, by clear switch action, or by removal of power. Specific guidance for clearing special types of semiconductor (electronic) memories will be provided by the CSO. Clearance actions will be verified, where feasible, to ensure that all applicable portions of memory have been cleared.

c. Other Storage Media. Other storage media such as magnetic tapes, * disks and drums on which classified information have been recorded may be * cleared by overwriting once with unclassified information. Clearance * actions will be appropriately verified, where feasible, and recorded. * Selective overwriting of storage media is permissible only when the exact * storage locations of classified information are known, those locations can * be overwritten, that action can be verified. Media which have been cleared * may be used for recording information with a lower classification level or * unclassified, but such media must be provided continuous protection as * described in paragraph 106e until appropriately declassified pursuant to * paragraph 116. *

d. Equipment. Any equipment or device physically handling classified media or material shall be visually examined as a part of the process of clearing the equipment. This provision is applicable, but not limited, to such devices as card readers and punches, optical and magnetic-ink character recognition systems, paper tape readers and punches, computer output microfilmers, printers, plotters and so on. This will require appropriate physical and visual examination of the normal media path through the particular equipment to detect the possible presence of media. An examination of the equipment must include a search of the locations where media or material may have become lodged. Equipment access panels and/or other removable components may have to be removed or opened to perform the inspection. Where the equipment contains internal memory or other storage media which have been used to store information, these media shall be cleared as in paragraph b or c above.

116. Media and Equipment Declassification.

a. Special precautions must be taken before systems, storage media or equipment and devices containing storage media can be released from classified material safeguarding controls. To release such media or computer hardware, appropriate actions must be taken to ensure that all classified information has been totally eradicated, that is, the storage media must be declassified. After the storage media have been properly declassified, the media, or the hardware containing the media, may be handled as unclassified material provided that all markings indicating its use for classified processing are removed. Where feasible, each declassification action must be verified (at least randomly) to ensure that all classified information contained on the media has been destroyed. When media are declassified, a record of media declassification must be completed. In the case of accountable media, this requirement can be met by completing the accountability record to indicate the declassification action taken, the date and the persons taking the action. For other storage media and computer hardware containing storage media for which there is no accountability record, declassification and release records must be created for the particular media, device or equipment are retained by the contractor for a period of 3 years if previously used for TOP SECRET, 2 years if previously used for SECRET, and 1 year if previously used for CONFIDENTIAL.

b. Most magnetic storage media can be declassified by the use of approved degaussing equipment and devices. The CSO will advise the contractor of currently approved: (i) electrical magnetic tape degaussers to declassify reels of magnetic tape, to include "high energy" tape with a *
coercivity less than 750 oersteds, (ii) adapters for electrical tape *
degaussers to declassify flexible (floppy) disks, tape cassettes and magnetic cards, (iii) floppy disk degaussers, and (iv) hand-held permanent magnetic devices for declassifying disk and drum surfaces. The contractor shall establish procedures to ensure strict compliance with the manufacturer's instructions for operating the degaussing equipment and to ensure continuing effectiveness of the equipment. It should be noted that tape degaussers are not authorized for declassifying "high-energy" magnetic *
recording tape with a coercivity greater than 750 oersteds. High-energy *
magnetic tape which is more commonly used to record analog, audio, video and *

other non-digital information shall have a distinguishing label applied to the reel which identifies the coercivity and identify it as "high-energy." "High-energy" tape with a coercivity of 750 oersteds or greater shall be safeguarded until its physical destruction. *

c. Specific guidance for declassification and verification of particular types of memory and storage media is available from the CSO. Instructions regarding the declassification and/or disposition of media containing COMSEC or special access program material should be provided by the contracting activity. Authorized procedures for declassification of the most commonly used memories and storage media are as follows:

(1) Volatile semiconductor memory can be declassified by overwriting each memory location with any character pattern, or by the removal of main and any backup power from the system. Non-volatile semiconductor memory may be declassified in accordance with procedures available from the CSO. *

(2) Magnetic core memory used in the processing of information classified no higher than SECRET can be declassified by overwriting each addressable memory location alternately with any pattern of bits and then with its complementary or opposite bit pattern (for example, binary ones and then binary zeros) for 100 changes of state. The same procedure applies for the declassification of core memory used for processing TOP SECRET information, except that the memory must be overwritten for 1000 changes of state.

(3) Reels of magnetic tape can be declassified by the use of an approved electrical tape degausser.

(4) Tape cassettes can be declassified by using an approved electrical tape degausser with the appropriate adapter.

(5) Flexible (floppy) disks and diskettes can be declassified by:

(a) using an approved floppy disk degausser,

(b) using an approved electrical tape degausser with the appropriate adapter, or

(c) exposing the recording surfaces to an approved hand-held permanent magnet.

(6) Disk packs, disk platters, drums and similar rigid magnetic storage devices can be declassified by:

(a) exposing the recording surfaces to an approved hand-held permanent magnet, or

(b) overwriting all data storage locations alternately with any pattern of bits and then with its complementary or opposite bit * pattern (for example, binary ones and then binary zeros) followed by a final overwrite with any other characters or bit pattern. Unclassified information used in the final overwrite shall be left on the device. Selective overwriting of storage media is authorized only when the exact storage locations of classified information are known, those locations can be overwritten as required and that action can be verified. * *

(7) Magnetic cards can be declassified by using an approved electrical tape degausser with the appropriate adapter.

(8) Cathode ray tube (CRT) screen surfaces shall be inspected and/or tested to detect evidence of burned-in information. If the inspection reveals classified information etched into the phosphor, the CRT device shall be retained within the appropriate security environment, or the screen itself shall be destroyed. In the absence of burned-in classified information, the CRT may be handled as unclassified.

Section XIV. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

117. Policy. The sensitivity of CNWDI is such that it is in the national interest to ensure that access is granted to the absolute minimum number of employees who require it for the accomplishment of assigned responsibilities on the strictest need-to-know basis. The FSO shall be responsible for ensuring that access to CNWDI is limited on a strict need-to-know basis within the facility. The top management official shall ensure that the need-to-know principle is strictly enforced. Management personnel at all levels will be responsible for ensuring that requests for access to CNWDI are not automatically approved. Full and complete justification must be made before any employee is authorized for access to CNWDI. Because of the importance of such information to our national policies, special procedures have been established for its control.

118. Access Requirements. A final TOP SECRET or SECRET PCL, granted in accordance with paragraph 24a(1), is valid for access to CNWDI of the same or lesser security classification, provided the employee has been given a security briefing, in accordance with paragraph 119. In rare instances, an immigrant alien who possesses a unique or very unusual talent or skill that is essential to the U.S. Government, and is not possessed to a comparable degree by an available U.S. citizen, may be authorized for access to CNWDI only. In such cases a request with full justification shall be forwarded to the contracting officer. If access to CNWDI is approved for the immigrant alien, such approval is limited to the specific contract of the UA, and is not valid for access to CNWDI on other contracts.

119. Briefings. Employees having a need for access to CNWDI shall be briefed on its sensitivity by the FSO or his or her alternate. The briefing shall include the definition of CNWDI, a reminder as to the extreme sensitivity of the information, and an explanation of the individual's continuing responsibility for properly safeguarding CNWDI and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a specific need-to-know for the particular information. The briefing shall also be tailored to cover any local special requirements.

120. Records. The contractor shall maintain a record of all employees who have been authorized access to CNWDI, and the date on which such employees were briefed. These records will be maintained in a manner that will facilitate verification, and shall be retained for 3 years following the termination of employment and/or the termination of the individual's clearance, as applicable.

121. Marking. In addition to other markings required by this manual, documents, including working papers, sound, voice, or electronic records, and any other media, which contain CNWDI and are generated after September 1, 1978, shall be clearly marked, "Critical Nuclear Weapon Design Information -- DoD Directive 5210.2 Applies." Documents shall be marked on the cover, title page, lead page, and the back cover. Similar documents and other media published before September 1, 1978 that are in working files will be

similarly marked (substantially as provided above) to indicate they contain CNWDI information. In addition, paragraphs of documents generated after September 1, 1978 that contain CNWDI will be so marked. (Example: (SRD)(N).) An (N) following the classification denotes that the classified material is additionally identified as CNWDI.

122. Subcontracting and Consultants. The contractor shall not award a subcontract which would necessitate access to CNWDI without the prior written approval of the contracting officer. This approval may be included on the DD Form 254. Type A Consultants may be briefed and afforded access to CNWDI, but such access may be permitted only at the facility of the contractor who engaged the Type A Consultant or at the government contracting activity. Type B and C Consultants shall not be briefed or afforded access to CNWDI without the prior approval of the contracting officer.

123. Transmission Outside the Facility. Transmission outside the facility is authorized only to the contracting activity, a prime contractor, or a subcontractor approved pursuant to paragraph 122. Any other transmission must be approved by the contracting officer. In addition, prior to transmission to another cleared facility, the contractor shall verify from the CSO of the recipient facility that the facility has been authorized for access to CNWDI. When CNWDI is transmitted to another facility, the inner wrapping will be addressed to the personal attention of the FSO or his or her alternate, and in addition to any other prescribed markings on the inner wrapping will be the marking, "Critical Nuclear Weapon Design Information -- DoD Directive 5210.2 Applies." Similarly, transmissions addressed to the contracting activity or other U.S. Government agency shall bear on the inner wrapper the marking, "Critical Nuclear Weapon Design Information -- DoD Directive 5210.2 Applies."

Section XV. OPERATIONS SECURITY (OPSEC)

124. Purpose. This section of the manual provides information and guidance for uniform implementation of the DoD OPSEC program when contractually imposed on contractors participating in the Defense Industrial Security Program.

125. General. OPSEC is a DoD directed effort. Its principal objective is to preclude the disclosure of classified information by denying or reducing the opportunity of hostile intelligence services (HOIS) to gain access by directly observing/analyzing/evaluating our activities and operations, the awareness of which may lead to the compromise of classified information. Stated another way, OPSEC is the process of denying adversaries information about friendly intentions, capabilities, plans and programs by identifying, controlling, and protecting intelligence information and indicators associated with planning and conducting military operations as well as other defense activities not already afforded adequate protection as classified information.

a. The general aim of OPSEC is to promote mission effectiveness by preserving essential secrecy about U.S. intentions, capabilities, and current activities when the DISP procedures for safeguarding classified material and information require enhancement. Secrecy essential to defense activities may be compromised whenever open sources (such as technical articles, press releases, National Technical Information Service publications, the Congressional Record, Commerce Business Daily, or contract awards) and detectable activities (such as communications, logistics actions, research, development and test activities, or radar emissions) provide information that hostile intelligence can piece together or analyze, resulting in adversary actions harmful to U.S. interests. In some instances, such information or indicators/activities are unprotected or not addressed by the DISP requirements for classified material and require case-by-case planning to identify them. The fundamental goal of the OPSEC process is to minimize or eliminate such indicators. OPSEC thus encompasses activities which are unique to the OPSEC process, i.e., (a) determining, through threat/vulnerability analysis, whether there are unacceptable/undesirable intelligence indicators and what they are; (b) developing and implementing countermeasures to best eliminate or minimize them.

b. OPSEC uses the same security measures that have been used to protect government information for years under the DISP but adds a new dimension. This new dimension or emphasis is the security of unclassified intelligence indicators. It is the protection of things we do, our operations, tests, and activities. As such, OPSEC is intended to complement the DISP.

126. Applicability. The DoD OPSEC program is applicable only to Defense contractors participating in the DISP when the contracting User Agency determines that additional OPSEC measures are essential to protect classified information for specific classified contracts and imposes OPSEC as a contractual requirement. OPSEC is concerned with all sources of exploitable information. The DISP generally covers only the classified

information disclosure problem, while OPSEC covers the total problem by addressing vulnerabilities and countermeasures for a specific program. OPSEC is principally oriented to those instances in which evaluations indicate program weaknesses which could lead to the disclosure of classified information.

a. OPSEC will be directed to the protection of unclassified intelligence indicators on classified programs of such a nature that the disclosure of the indicators may lead to the compromise of classified information. OPSEC is not intended as a vehicle to protect unclassified technology; other programs exist to protect this information (DoD Directive 5230.25).

b. Specific detailed UA requirements for OPSEC shall be included in appropriate requisition documentation and resultant contract or addendum thereto in sufficient detail to ensure complete contractor understanding of exactly what special OPSEC provisions or measures are required by the UA. Full disclosure of these requirements is essential so that contractors can comply and charge attendant costs to the specific contracts which have OPSEC provisions. In providing such measures, UAs shall not solely refer to their internal regulations when imposing OPSEC requirements, but shall fully specify the particulars in the contract proper and shall provide necessary information to fully explain internal regulations. Additionally, applicable DD 254s will be annotated to indicate that OPSEC requirements are contained in the contract or addendum thereto.

c. Contractual OPSEC requirements shall be strictly limited to those sensitive projects which clearly justify extraordinary security measures beyond those embodied in the DISP as outlined in the ISM. If the ISM provides a countermeasure or safeguard for a particular identified vulnerability concern, the ISM will be allowed to address it and redundant countermeasures will not be added as contractual OPSEC requirements (e.g. physical, information or personnel security). UAs will make this determination prior to imposing OPSEC measures.

d. Full and detailed OPSEC contract and subcontract requirements to include DD 254s will be provided to DIS CSOs by UAs or prime contractors as appropriate.

e. When requested by the installation commander, DIS will perform OPSEC inspections of contractor facilities located on military installations. At contractor facilities not located on military installations, DIS has principal responsibility for inspecting contractor compliance with OPSEC requirements. Cognizant UA representatives may accompany DIS if requested. OPSEC inspections will be accomplished:

(1) As part of a regularly scheduled industrial security inspection.

(2) As part of an unannounced industrial security inspection.

127. Procedures for Self-Inspecting OPSEC Programs.

As will be the case with CSOs, contractors shall use the detailed information provided them by the contracting activity as the basis for OPSEC self-inspections.

Appendix I. INDUSTRIAL SECURITY FORMS

A. Application. The purpose of this appendix is to describe the forms used by DoD contractors in industrial security matters, and to provide instructions for the use and completion of each of these forms. A sample of each form is included. These forms shall not be used for any purpose or in any other manner, except as provided for in this manual or for training purposes.

B. Special Privacy Section Instructions. The privacy section instructions on DD Forms 48, 49 and 48-3 are no longer applicable. (New personnel security questionnaires, when published, will contain no special privacy instructions.) Each employee will be advised that if they believe there is a significant personal matter which they desire not to disclose to their employer, they may request an interview with a Defense Investigative Service agent by entering "DIS Interview Requested" rather than completing the specific item.

C. "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" (DD Form 48). This form is used to obtain personal data from a U.S. citizen being considered for a DoD CONFIDENTIAL or SECRET PCL. The form is prepared jointly by management and the person being considered for the clearance. The completion of this form shall not be required, except when the person concerned is being processed for a clearance. The completed form should be forwarded to the DISCO, P.O. Box 2499, Columbus, Ohio 43216-5006. Forms that pertain to OODEPs and are submitted in conjunction with the FCL application shall be appropriately marked "OODEP" in item e of the (To be Completed by Employer) section in lieu of the contract number. * *

SAMPLE

DDForm 48

PERSONNEL SECURITY QUESTIONNAIRE
INDUSTRIAL - NAC
DD FORM 48

PRIVACY ACT STATEMENT

AUTHORITY: Internal Security Act of 1950 and Executive Order 10865, as amended by Executive Order 10909; Executive Order 9397, November 1943 (SSN).

PRINCIPAL PURPOSES: To obtain background information for personnel security investigative and evaluative purposes in order to determine the security eligibility of Department of Defense contractors and employees of Department of Defense contractors for (1) access to classified information, or (2) assignment to a sensitive position.

ROUTINE USES: (1) Determine the scope of a personnel security investigation.

(2) Provide evaluators or adjudicators with personal history information relevant to personnel security determinations.

The information may be disclosed to other Federal agencies that are authorized under specific statutory or Executive authority to make personnel security determinations.

A copy of the report of personnel security investigation will be maintained by the Personnel Investigations Center of the Defense Investigative Service and may be used in future security clearance determinations. You have the right to obtain a copy of the report of investigation and/or request amendment to the file.

DISCLOSURE: Voluntary; however, failure to furnish all or part of the information requested may result in (1) denial of access to classified information, or (2) non-selection for assignment to a sensitive position. Disclosure of your Social Security Number is necessary to fulfill requirements of the above cited authorities. It is intended that this notice be retained for personal records.

GENERAL INSTRUCTIONS

THE PERSONNEL SECURITY QUESTIONNAIRE (PSQ) IS AN IMPORTANT DOCUMENT AND MUST BE COMPLETED WITHOUT MISSTATEMENT OR OMISSION OF IMPORTANT FACTS. ALL ENTRIES ARE SUBJECT TO VERIFICATION BY INVESTIGATION.

- THE FORM MUST BE TYPED OR PRINTED.
- COMPLETE ITEMS 1-13, SIGN THE FORM AT THE BOTTOM, AND THEN PROVIDE THE FORM TO YOUR EMPLOYER WHO WILL REVIEW IT TO ASSURE THAT ENTRIES ARE COMPLETE AND CORRECT. AFTER THE FORM IS RETURNED TO YOU, PROCEED TO COMPLETE 14-18 OF THE PRIVACY SECTION.
- IF ADDITIONAL SPACE IS REQUIRED FOR ANY ITEM, ATTACH ADDITIONAL SHEETS OF PLAIN WHITE PAPER. WHEN ATTACHING ADDITIONAL SHEETS ALWAYS IDENTIFY THE ITEM NUMBER BEING CONTINUED AND FOLLOW THE FORMAT FOR ENTERING INFORMATION PRESCRIBED ON THE FORM AND IN THE DETAILED INSTRUCTIONS.
- ALL QUESTIONS MUST BE ANSWERED. IF AN ITEM IS NOT APPLICABLE INDICATE "NOT APPLICABLE" OR "N/A." DO NOT USE THE TERM "UNKNOWN" FOR DATES OF EMPLOYMENT OR RESIDENCE. IF THIS INFORMATION IS NOT KNOWN PRECISELY, GIVE THE DATE AS BEST YOU CAN RECALL FOLLOWED BY APPROPRIATE QUALIFYING LANGUAGE, E.G., "DATE ESTIMATED" OR "APPROX."
- UNLESS OTHERWISE SPECIFIED:
  - ALL DATES SHOULD BE ENTERED IN TERMS OF YEAR AND MONTH USING THE LAST TWO DIGITS OF THE YEAR AND A TWO DIGIT NUMBER REPRESENTING THE MONTH, E.G., JANUARY 1987 WOULD BE ENTERED AS 87-01 AND DECEMBER 1987 WOULD BE ENTERED AS 87-12.
  - NAMES OF PERSONS SHOULD BE ENTERED IN THE FOLLOWING ORDER: LAST NAME, FIRST NAME AND MIDDLE INITIAL.
  - ADDRESSES SHOULD INCLUDE THE NUMBER AND STREET, CITY, STATE OR COUNTRY, AND ZIP CODE.
- BEFORE ENTERING ANY INFORMATION ON THE FORM, READ CAREFULLY THE DETAILED INSTRUCTIONS PROVIDED WITH THE FORM. IF AT ANY TIME DURING COMPLETION OF THE FORM, A QUESTION ARISES THAT DOES NOT APPEAR TO BE COVERED BY THE DETAILED INSTRUCTIONS, CONTACT THE INDIVIDUAL OR OFFICE THAT PROVIDED YOU WITH THE FORM.
- ONCE THE FORM HAS BEEN COMPLETED, PLACE IT IN THE PRE-ADDRESSED ENVELOPE THAT HAS BEEN PROVIDED, TOGETHER WITH THE COMPLETED FD 258 (FINGERPRINT CARD). SEAL THE ENVELOPE, SIGN ACROSS THE ENVELOPE FLAP ON THE LINE PROVIDED AND AFFIX THE DATE OF SIGNATURE. DELIVER THE SEALED ENVELOPE TO YOUR EMPLOYER IMMEDIATELY.

DD Form 48 Instructions, JUL 87

SAMPLE
DD Form 48
Page Two

DEPARTMENT OF DEFENSE
PERSONNEL SECURITY QUESTIONNAIRE (Industrial-NAC)

Form Approved
OMB No. 0704-0005
Expires May 31, 1990

1.a LAST NAME—FIRST NAME—MIDDLE NAME	b. MAIDEN NAME *(If any)*	DATE
		FOR DIS USE ONLY

2. ALIASES	3.a SEX	☐ Male ☐ Female	b. RACE	4. SOCIAL SECURITY NUMBER

5. DATE OF BIRTH *(Year-Month-Day)*	6. PLACE OF BIRTH			
	a. CITY	b. COUNTY	c. STATE	d. COUNTRY

7.a U.S. CITIZEN	b. NATIVE	c. IF NATURALIZED, CERTIFICATE NO.(s)	d. IF DERIVED, PARENT(s) CERTIFICATE NO.(s)	e. DATE	f. PLACE	g. COURT
☐ Yes ☐ No	☐ Yes ☐ No					

h. DUAL CITIZEN ☐ Yes ☐ No *(If "Yes" see DETAILED INSTRUCTIONS.)*

8. MILITARY SERVICE *(Include Reserve/National Guard.)*

a. FROM	b. TO	c. BRANCH	d. RANK	e. SERVICE NO.(s)	f. COUNTRY

9. PREVIOUS CLEARANCE DATA	Yes	No
a. Have you ever been granted a security clearance? *(If "Yes" give details below.)*		

LEVEL	DATE GRANTED	GRANTED BY	NAME OF EMPLOYER

	Yes	No
b. Have you ever terminated employment while request for security clearance was pending? *("Yes" answer must be explained in accordance with the DETAILED INSTRUCTIONS.)*		

10. FAMILY/ASSOCIATES *(See DETAILED INSTRUCTIONS for persons to be listed.)*

a. RELATIONSHIP AND NAME	b. DATE OF BIRTH	c. PLACE OF BIRTH	d. ADDRESS	e. CITIZENSHIP
FATHER				
MOTHER *(Maiden Name)*				
SPOUSE *(Maiden Name)*				
FORMER SPOUSE				

11. RESIDENCES *(Begin with current address-See DETAILED INSTRUCTIONS.)*

a. DATES (Yr & Mo)		b. NUMBER AND STREET	c. CITY	d. STATE	e. ZIP CODE
FROM	TO				
	Present				

12. EMPLOYMENT *(Include self-employment, part-time employment and/or unemployment.) (See DETAILED INSTRUCTIONS.)*

a. DATES (Yr & Mo)		b. NAME OF EMPLOYER	c. ADDRESS	d. ZIP CODE	e. SUPERVISOR
FROM	TO				
	Present				

13. FEDERAL SERVICE, FOREIGN TRAVEL/CONNECTIONS *(If "Yes" see DETAILED INSTRUCTIONS.)*	Yes	No
a. Have you ever been in the Federal Civil Service?		
b. Have you traveled or resided abroad for other than the U.S. Government?		
c. Do you have any foreign property or business connections or have you ever been employed by or acted as a consultant or representative for a foreign government, firm, or agency?		

TO BE COMPLETED BY EMPLOYER a. LEVEL OF CLEARANCE ☐ Secret ☐ Confidential

b. CITIZENSHIP VERIFIED ☐ Yes ☐ No c. JOB TITLE

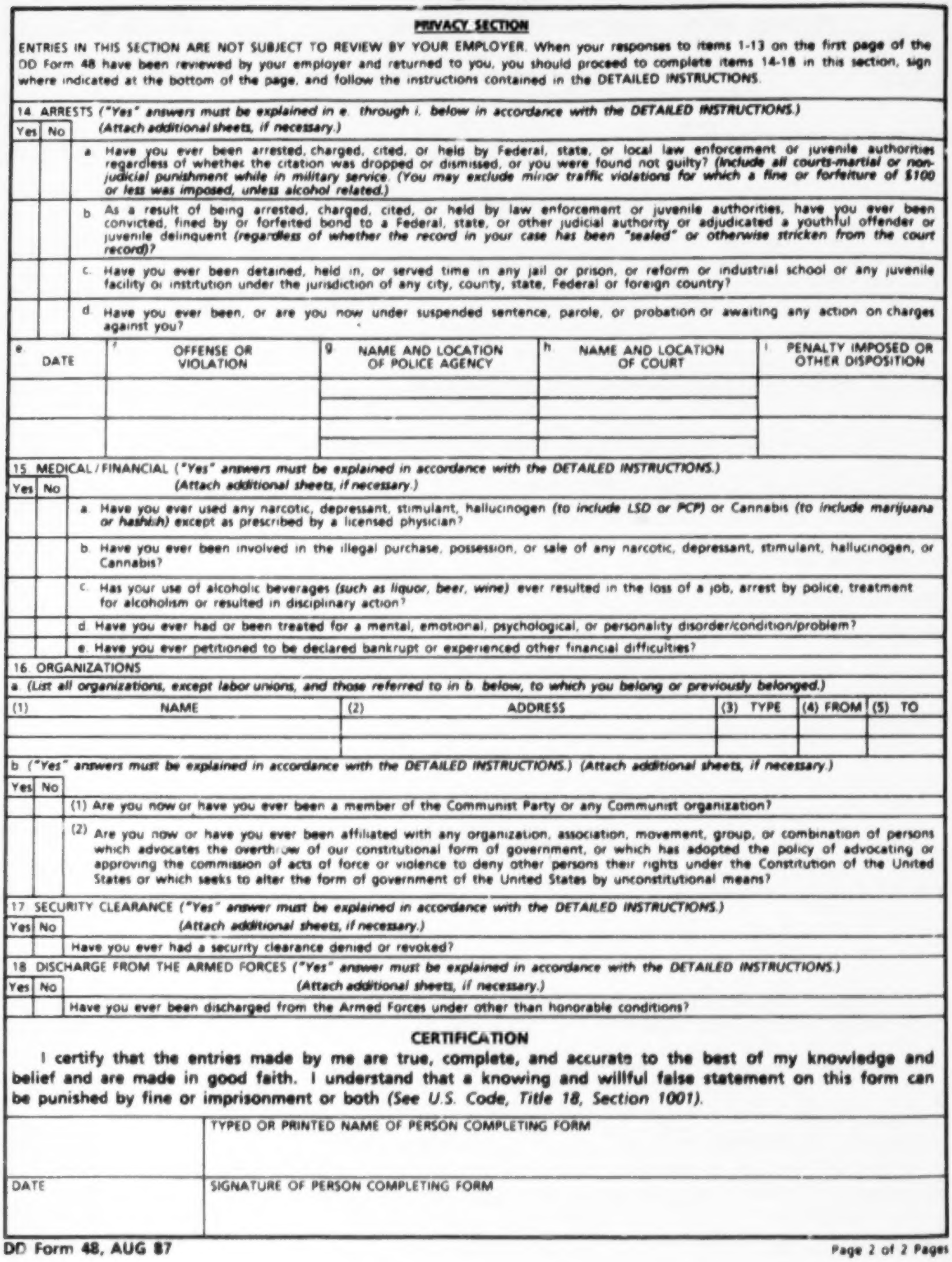
d. COMMERCIAL AND GOVERNMENT ENTITY CODE e. CONTRACT NUMBER

f. CERTIFICATION - I certify that the above named individual is employed by this company and has the need for the clearance indicated to perform on classified contracts.

DATE SIGNED	SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE	TELEPHONE NO

DD Form 48, AUG 87 *Previous editions are obsolete.* Page 1 of 2 Pages

SAMPLE
DD Form 48
Page Three



PRIVACY SECTION

ENTRIES IN THIS SECTION ARE NOT SUBJECT TO REVIEW BY YOUR EMPLOYER. When your responses to items 1-13 on the first page of the DD Form 48 have been reviewed by your employer and returned to you, you should proceed to complete items 14-18 in this section, sign where indicated at the bottom of the page, and follow the instructions contained in the DETAILED INSTRUCTIONS.

14. ARRESTS *("Yes" answers must be explained in e. through i. below in accordance with the DETAILED INSTRUCTIONS.)* *(Attach additional sheets, if necessary.)*

Yes	No	
		a. Have you ever been arrested, charged, cited, or held by Federal, state, or local law enforcement or juvenile authorities regardless of whether the citation was dropped or dismissed, or you were found not guilty? *(Include all courts-martial or non-judicial punishment while in military service. (You may exclude minor traffic violations for which a fine or forfeiture of $100 or less was imposed, unless alcohol related.)*
		b. As a result of being arrested, charged, cited, or held by law enforcement or juvenile authorities, have you ever been convicted, fined by or forfeited bond to a Federal, state, or other judicial authority or adjudicated a youthful offender or juvenile delinquent *(regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record)*?
		c. Have you ever been detained, held in, or served time in any jail or prison, or reform or industrial school or any juvenile facility or institution under the jurisdiction of any city, county, state, Federal or foreign country?
		d. Have you ever been, or are you now under suspended sentence, parole, or probation or awaiting any action on charges against you?

e. DATE	f. OFFENSE OR VIOLATION	g. NAME AND LOCATION OF POLICE AGENCY	h. NAME AND LOCATION OF COURT	i. PENALTY IMPOSED OR OTHER DISPOSITION

15. MEDICAL / FINANCIAL *("Yes" answers must be explained in accordance with the DETAILED INSTRUCTIONS.)* *(Attach additional sheets, if necessary.)*

Yes	No	
		a. Have you ever used any narcotic, depressant, stimulant, hallucinogen *(to include LSD or PCP)* or Cannabis *(to include marijuana or hashish)* except as prescribed by a licensed physician?
		b. Have you ever been involved in the illegal purchase, possession, or sale of any narcotic, depressant, stimulant, hallucinogen, or Cannabis?
		c. Has your use of alcoholic beverages *(such as liquor, beer, wine)* ever resulted in the loss of a job, arrest by police, treatment for alcoholism or resulted in disciplinary action?
		d. Have you ever had or been treated for a mental, emotional, psychological, or personality disorder/condition/problem?
		e. Have you ever petitioned to be declared bankrupt or experienced other financial difficulties?

16. ORGANIZATIONS

a. *(List all organizations, except labor unions, and those referred to in b. below, to which you belong or previously belonged.)*

(1) NAME	(2) ADDRESS	(3) TYPE	(4) FROM	(5) TO

b. *("Yes" answers must be explained in accordance with the DETAILED INSTRUCTIONS.) (Attach additional sheets, if necessary.)*

Yes	No	
		(1) Are you now or have you ever been a member of the Communist Party or any Communist organization?
		(2) Are you now or have you ever been affiliated with any organization, association, movement, group, or combination of persons which advocates the overthrow of our constitutional form of government, or which has adopted the policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States or which seeks to alter the form of government of the United States by unconstitutional means?

17. SECURITY CLEARANCE *("Yes" answer must be explained in accordance with the DETAILED INSTRUCTIONS.)* *(Attach additional sheets, if necessary.)*

Yes	No	
		Have you ever had a security clearance denied or revoked?

18. DISCHARGE FROM THE ARMED FORCES *("Yes" answer must be explained in accordance with the DETAILED INSTRUCTIONS.)* *(Attach additional sheets, if necessary.)*

Yes	No	
		Have you ever been discharged from the Armed Forces under other than honorable conditions?

CERTIFICATION

I certify that the entries made by me are true, complete, and accurate to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both *(See U.S. Code, Title 18, Section 1001)*.

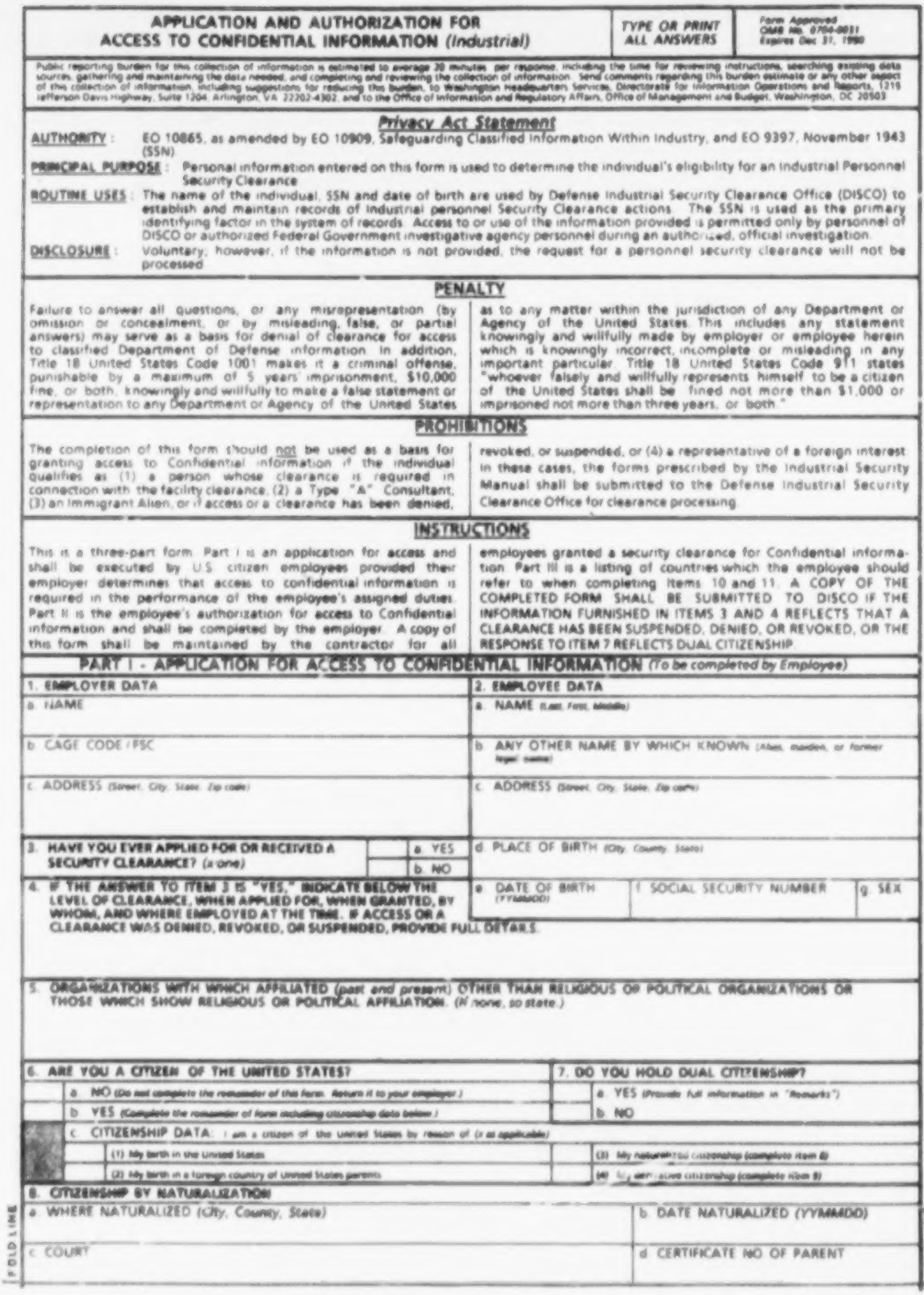
	TYPED OR PRINTED NAME OF PERSON COMPLETING FORM
DATE	SIGNATURE OF PERSON COMPLETING FORM

DD Form 48, AUG 87 — Page 2 of 2 Pages

D. "Application and Authorization for Access to Confidential Information (Industrial)" (DD Form 48-2). This form is used to obtain personal data from a U.S. citizen being considered for a CONFIDENTIAL PCL by a contractor. The form is prepared jointly by the person being considered for the clearance and by the contractor. Completion of this form is a prerequisite to the granting of a CONFIDENTIAL clearance by a contractor.

SAMPLE

DD Form 48-2



APPLICATION AND AUTHORIZATION FOR ACCESS TO CONFIDENTIAL INFORMATION *(Industrial)*	*TYPE OR PRINT ALL ANSWERS*	Form Approved OMB No. 0704-0031 Expires Dec 31, 1990

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503.

Privacy Act Statement

AUTHORITY: EO 10865, as amended by EO 10909, Safeguarding Classified Information Within Industry, and EO 9397, November 1943 (SSN).

PRINCIPAL PURPOSE: Personal information entered on this form is used to determine the individual's eligibility for an Industrial Personnel Security Clearance.

ROUTINE USES: The name of the individual, SSN and date of birth are used by Defense Industrial Security Clearance Office (DISCO) to establish and maintain records of Industrial personnel Security Clearance actions. The SSN is used as the primary identifying factor in the system of records. Access to or use of the information provided is permitted only by personnel of DISCO or authorized Federal Government investigative agency personnel during an authorized, official investigation.

DISCLOSURE: Voluntary, however, if the information is not provided, the request for a personnel security clearance will not be processed.

PENALTY

Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18 United States Code 1001 makes it a criminal offense, punishable by a maximum of 5 years' imprisonment, $10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement knowingly and willfully made by employer or employee herein which is knowingly incorrect, incomplete or misleading in any important particular. Title 18 United States Code 911 states "whoever falsely and willfully represents himself to be a citizen of the United States shall be fined not more than $1,000 or imprisoned not more than three years, or both."

PROHIBITIONS

The completion of this form should not be used as a basis for granting access to Confidential information if the individual qualifies as (1) a person whose clearance is required in connection with the facility clearance, (2) a Type "A" Consultant, (3) an Immigrant Alien, or if access or a clearance has been denied, revoked, or suspended, or (4) a representative of a foreign interest. In these cases, the forms prescribed by the Industrial Security Manual shall be submitted to the Defense Industrial Security Clearance Office for clearance processing.

INSTRUCTIONS

This is a three-part form. Part I is an application for access and shall be executed by U.S. citizen employees provided their employer determines that access to confidential information is required in the performance of the employee's assigned duties. Part II is the employee's authorization for access to Confidential information and shall be completed by the employer. A copy of this form shall be maintained by the contractor for all employees granted a security clearance for Confidential information. Part III is a listing of countries which the employee should refer to when completing Items 10 and 11. A COPY OF THE COMPLETED FORM SHALL BE SUBMITTED TO DISCO IF THE INFORMATION FURNISHED IN ITEMS 3 AND 4 REFLECTS THAT A CLEARANCE HAS BEEN SUSPENDED, DENIED, OR REVOKED, OR THE RESPONSE TO ITEM 7 REFLECTS DUAL CITIZENSHIP.

PART I - APPLICATION FOR ACCESS TO CONFIDENTIAL INFORMATION *(To be completed by Employee)*

1. EMPLOYER DATA	**2. EMPLOYEE DATA**
a. NAME	a. NAME *(Last, First, Middle)*
b. CAGE CODE / FSC	b. ANY OTHER NAME BY WHICH KNOWN *(Alias, maiden, or former legal name)*
c. ADDRESS *(Street, City, State, Zip code)*	c. ADDRESS *(Street, City, State, Zip code)*
3. HAVE YOU EVER APPLIED FOR OR RECEIVED A SECURITY CLEARANCE? *(x one)* ☐ a. YES ☐ b. NO	d. PLACE OF BIRTH *(City, County, State)*
4. IF THE ANSWER TO ITEM 3 IS "YES," INDICATE BELOW THE LEVEL OF CLEARANCE, WHEN APPLIED FOR, WHEN GRANTED, BY WHOM, AND WHERE EMPLOYED AT THE TIME. IF ACCESS OR A CLEARANCE WAS DENIED, REVOKED, OR SUSPENDED, PROVIDE FULL DETAILS.	e. DATE OF BIRTH *(YYMMDD)* / f. SOCIAL SECURITY NUMBER / g. SEX

5. ORGANIZATIONS WITH WHICH AFFILIATED *(past and present)* **OTHER THAN RELIGIOUS OR POLITICAL ORGANIZATIONS OR THOSE WHICH SHOW RELIGIOUS OR POLITICAL AFFILIATION.** *(If none, so state.)*

6. ARE YOU A CITIZEN OF THE UNITED STATES?	**7. DO YOU HOLD DUAL CITIZENSHIP?**
☐ a. NO *(Do not complete the remainder of this form. Return it to your employer.)*	☐ a. YES *(Provide full information in "Remarks")*
☐ b. YES *(Complete the remainder of form including citizenship data below.)*	☐ b. NO

c. CITIZENSHIP DATA: *I am a citizen of the United States by reason of (x as applicable)*

☐ (1) My birth in the United States	☐ (3) My naturalized citizenship (complete item 8)
☐ (2) My birth in a foreign country of United States parents	☐ (4) My derivative citizenship (complete item 9)

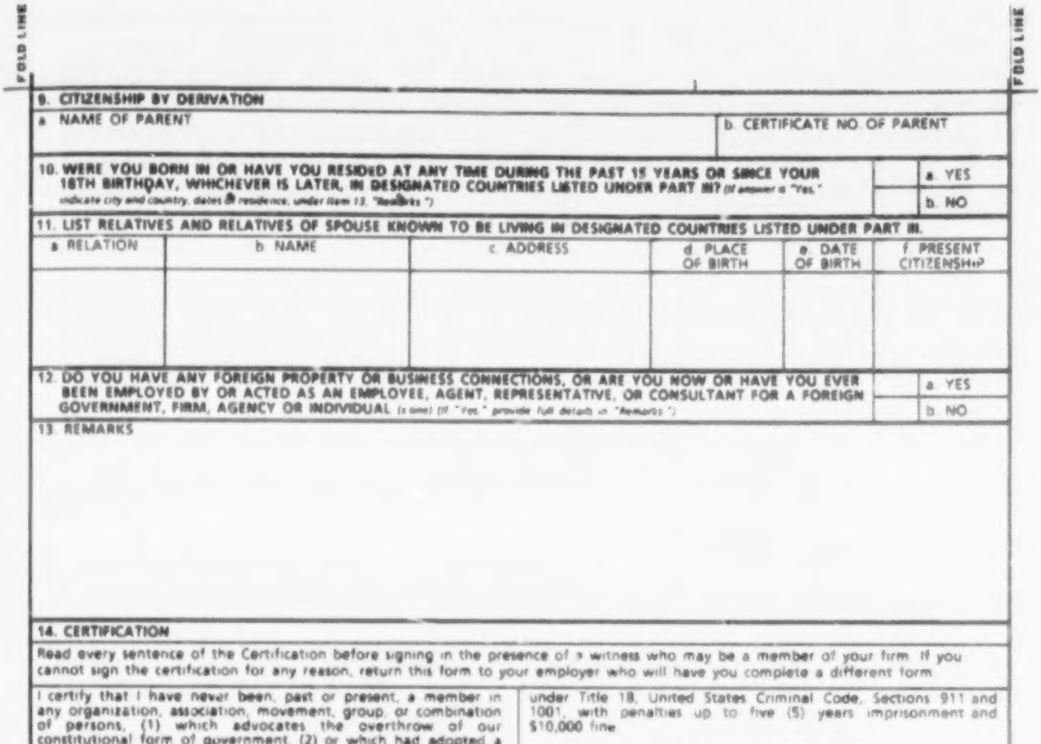
8. CITIZENSHIP BY NATURALIZATION

a. WHERE NATURALIZED (City, County, State)	b. DATE NATURALIZED (YYMMDD)
c. COURT	d. CERTIFICATE NO OF PARENT

FOLD LINE

FOLD LINE

DD Form 48-2
Page Two



FOLD LINE

FOLD LINE

9. CITIZENSHIP BY DERIVATION

a. NAME OF PARENT

b. CERTIFICATE NO. OF PARENT

10. WERE YOU BORN IN OR HAVE YOU RESIDED AT ANY TIME DURING THE PAST 15 YEARS OR SINCE YOUR 18TH BIRTHDAY, WHICHEVER IS LATER, IN DESIGNATED COUNTRIES LISTED UNDER PART III? *(If answer is "Yes," indicate city and country, dates of residence, under Item 13, "Remarks.")*

☐ a. YES

☐ b. NO

11. LIST RELATIVES AND RELATIVES OF SPOUSE KNOWN TO BE LIVING IN DESIGNATED COUNTRIES LISTED UNDER PART III.

a. RELATION	b. NAME	c. ADDRESS	d. PLACE OF BIRTH	e. DATE OF BIRTH	f. PRESENT CITIZENSHIP

12. DO YOU HAVE ANY FOREIGN PROPERTY OR BUSINESS CONNECTIONS, OR ARE YOU NOW OR HAVE YOU EVER BEEN EMPLOYED BY OR ACTED AS AN EMPLOYEE, AGENT, REPRESENTATIVE, OR CONSULTANT FOR A FOREIGN GOVERNMENT, FIRM, AGENCY OR INDIVIDUAL *(x one) (If "Yes," provide full details in "Remarks.")*

☐ a. YES

☐ b. NO

13. REMARKS

14. CERTIFICATION

Read every sentence of the Certification before signing in the presence of a witness who may be a member of your firm. If you cannot sign the certification for any reason, return this form to your employer who will have you complete a different form.

I certify that I have never been, past or present, a member in any organization, association, movement, group, or combination of persons, (1) which advocates the overthrow of our constitutional form of government, (2) or which had adopted a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, (3) or which seeks to alter the form of Government of the United States by unconstitutional means.

I certify that I know that any misrepresentation or false statement made by me herein may subject me to prosecution under Title 18, United States Criminal Code, Sections 911 and 1001, with penalties up to five (5) years imprisonment and $10,000 fine.

I certify that I am a citizen of the United States.

I certify that I have read and understand each sentence of this Certification.

I certify that the entries made by me on this form are true, complete, and correct to the best of my knowledge and belief, and are made in good faith.

a. SIGNATURE OF WITNESS

b. SIGNATURE OF PERSON MAKING CERTIFICATION

c. ADDRESS OF WITNESS *(City, County, State)*

d. DATE SIGNED

PART II - AUTHORIZATION FOR ACCESS TO CONFIDENTIAL INFORMATION *(To be completed by Employer)*

15. Whereas the Department of Defense has delegated to its contractors *(employers)* authority to grant access authorization for access to Confidential information to employees who require access in the performance of assigned duties; the undersigned, a duly authorized representative of the contractor, certifies that he/she has examined Part I of this form and the employment records pertaining to the employee executing Part I of this form, and has verified that the employee is a United States citizen; and that the employee may be granted a security clearance for Confidential information in accordance with the provisions of the Industrial Security Manual for Safeguarding Classified Information and such authorization is hereby granted this date.

16. AUTHORIZED EMPLOYER REPRESENTATIVE

a. TYPED NAME *(Last, First, Middle)*

b. TITLE

c. DATE SIGNED

d. SIGNATURE

17. DATE COMPLETED *(YYMMDD)*

PART III - LIST OF DESIGNATED COUNTRIES

Afghanistan; Albania; Angola; Berlin *(Soviet sector)*; Bulgaria; Cambodia *(Kampuchea)*; Cuba; Czechoslovakia; Democratic Peoples Republic of Korea *(North Korea)*; Democratic Republic of Vietnam; Ethiopia; German Democratic Republic *(GDR) (East Germany)*; Hungarian Peoples Repubic *(Hungary)*; Iran; Iraq; Kurile Islands and South Sakhalin *(Karafuto)*; Laos; Libyan Arab Republic; Mongolian Peoples Republic *(Outer Mongolia)*; Nicaragua; Peoples Republic of China *(Communist China) (including Tibet)*; Poland; Rumania; South Vietnam; Southern Yemen; Syria; Union of Soviet Socialist Republics *(USSR) (including Estonia, Latvia, Lithuania, and all other constituent republics)*; and Yugoslavia

DD Form 48-2, AUG 88 *Previous editions are obsolete.* 1498/215

E. "Department of Defense Personnel Security Questionnaire (Updating)" (DD
Form 48-3). This form is used to obtain current personal data to process *
a clearance action when an individual terminates employment with a con- *
tractor where his or her PCL had been granted and is subsequently reemployed *
by the contractor or another contractor in a capacity requiring access *
to classified information. Use of the DD Form 48-3 under this circumstance *
is prescribed if less than 24 months has elapsed since termination of the *
previously granted clearance. The DD Form 48-3 is also used in converting *
a UA clearance to an industrial security clearance and in reinstating a *
clearance that was administratively terminated. This form shall be pre- *
pared jointly by management and the individual being processed for the new *
clearance. The completed form shall be forwarded to DISCO, P.O. Box 2499, *
Columbus, Ohio, 43216-5006. Forms that pertain to OODEPs shall be appropri- *
ately marked "OODEP" in item 8 of Part I in lieu of the contract number. *

SAMPLE

DD Form 48-3

DEPARTMENT OF DEFENSE
PERSONNEL SECURITY QUESTIONNAIRE (Updating)

1. DATE FORM COMPLETED *(YYMMDD)*

Form Approved
OMB No. 0704-0005
Expires May 31, 1990

PENALTY: Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of 5 years imprisonment, $10,000 fine, or both, knowingly and willfully to make a false statement or representation to any Department or Agency of the United States as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly and willfully incorrect, incomplete or misleading in any important particular.

INSTRUCTIONS: One (1) copy of completed form will be submitted by the contractor when prescribed by the Industrial Security Manual for Safeguarding Classified Information to request transfer of clearance. Type or print all answers; form will not be accepted unless completely and properly executed. Use blank sheets for additional information, identifying by item number. Questions which do not apply will be marked "None."

INSTRUCTIONS TO EMPLOYEE: This form is in three parts. Part I must be completed by your employer before you complete the other parts. You must complete Part III in private. Before filling in any part, you should familiarize yourself with all questions. Do not sign this form without first reading the instructions in Part III.

PART I - TO BE COMPLETED BY EMPLOYER

1. TO:

DEFENSE INVESTIGATIVE SERVICE
DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE
BOX 2499
COLUMBUS, OHIO 43216-5006

2. NAME OF EMPLOYER *(If a subsidiary, include name of parent company)*

3. ADDRESS OF EMPLOYER *(Street, City, State, Zip Code)*

4. COMMERCIAL AND GOVERNMENT ENTITY CODE

5. JOB TITLE

6. CLEARANCE REQUESTED IS *(X one)*
☐ TRANSFER ☐ CONVERSION ☐ CONCURRENT

7. DESCRIPTION OF EMPLOYEE'S DUTIES WHICH REQUIRE ACCESS TO CLASSIFIED INFORMATION

8. CONTRACT NUMBER, WHEN APPLICABLE

9. SECURITY CLASSIFICATION OF MATERIALS OR INFORMATION EMPLOYEE WILL HAVE ACCESS TO

I CERTIFY THAT THE ENTRIES MADE BY ME ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF AND ARE MADE IN GOOD FAITH.

10a. SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE

b. TELEPHONE NO

PART II - TO BE COMPLETED BY EMPLOYEE

1. NAME *(Last, First, Middle)*

2. OTHER NAMES *(Indicate alias, maiden name, former legal name, etc)*

3. DATE OF BIRTH *(YYMMDD)*

4. SOCIAL SECURITY NUMBER

5. SEX

6. PLACE OF BIRTH *(City, State, Country)*

7. COUNTRY OF CITIZENSHIP

8a CURRENT RESIDENCE ADDRESS *(Street, City, State, or Other Political Subdivision, and Country)*

b. FROM *(Date - YYMMDD)*

9. LAST EMPLOYMENT AT WHICH CLEARANCE WAS GRANTED

a. POSITION HELD

b. DATES OF EMPLOYMENT *(YYMMDD)*
(1) FROM (2) TO

c. EMPLOYER NAME

d. EMPLOYER ADDRESS *(Street, City, State, Zip Code)*

10. CLEARANCE

a. LEVEL

b. DATE GRANTED *(YYMMDD)*

c. GRANTED BY

11. LIST EACH FOREIGN GOVERNMENT, FIRM, CORPORATION, OR PERSON FOR WHOM YOU ACT OR HAVE ACTED AS A REPRESENTATIVE, OFFICIAL OR EMPLOYEE IN THE PAST 5 YEARS. LIST ALL COMMUNIST GOVERNMENTS, FIRMS, OR CORPORATIONS FOR WHOM YOU HAVE EVER ACTED IN SUCH CAPACITY. ATTACH A STATEMENT FOR EACH AFFILIATION, AS REQUIRED BY PARAGRAPH 20 OF THE ISM

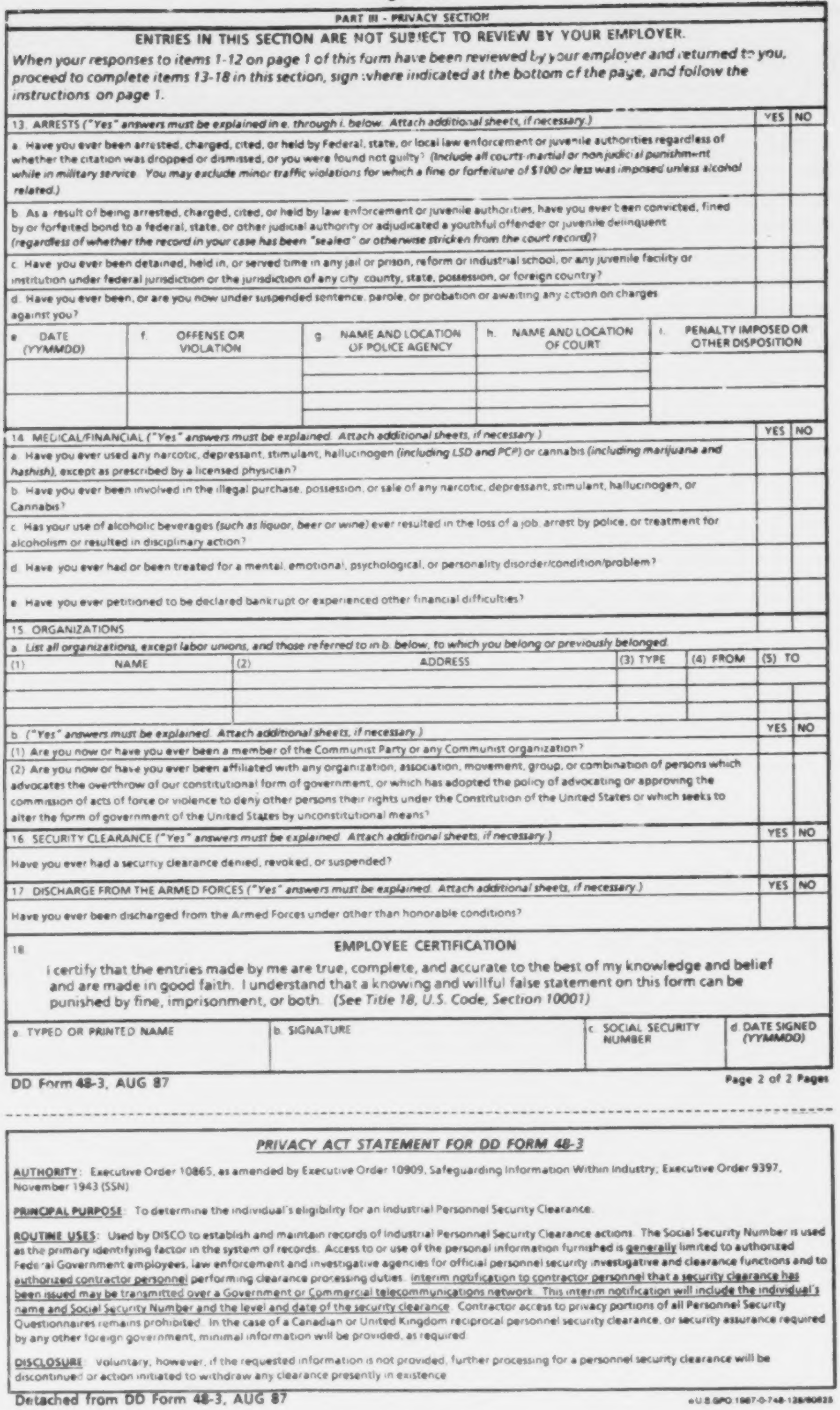
12. REMARKS

FURTHER INSTRUCTIONS: Do not complete PART III or the Certification at this time. After completing PART II return the form to your employer who will review it to assure that all entries are complete and the form is filled out properly. After your employer returns the forms to you, then start PART III and follow instructions on reverse side.

DD Form 48-3, AUG 87 *Previous editions are obsolete.* Page 1 of 2 Pages

SAMPLE

DD Form 48-3
Page Two



PART III - PRIVACY SECTION

ENTRIES IN THIS SECTION ARE NOT SUBJECT TO REVIEW BY YOUR EMPLOYER.

When your responses to items 1-12 on page 1 of this form have been reviewed by your employer and returned to you, proceed to complete items 13-18 in this section, sign where indicated at the bottom of the page, and follow the instructions on page 1.

	YES	NO
13. ARRESTS (*"Yes" answers must be explained in e. through i. below. Attach additional sheets, if necessary.*)		
a. Have you ever been arrested, charged, cited, or held by Federal, state, or local law enforcement or juvenile authorities regardless of whether the citation was dropped or dismissed, or you were found not guilty? *(Include all courts-martial or non judicial punishment while in military service. You may exclude minor traffic violations for which a fine or forfeiture of $100 or less was imposed unless alcohol related.)*		
b. As a result of being arrested, charged, cited, or held by law enforcement or juvenile authorities, have you ever been convicted, fined by or forfeited bond to a federal, state, or other judicial authority or adjudicated a youthful offender or juvenile delinquent *(regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record)*?		
c. Have you ever been detained, held in, or served time in any jail or prison, reform or industrial school, or any juvenile facility or institution under federal jurisdiction or the jurisdiction of any city, county, state, possession, or foreign country?		
d. Have you ever been, or are you now under suspended sentence, parole, or probation or awaiting any action on charges against you?		

e. DATE (YYMMDD)	f. OFFENSE OR VIOLATION	g. NAME AND LOCATION OF POLICE AGENCY	h. NAME AND LOCATION OF COURT	i. PENALTY IMPOSED OR OTHER DISPOSITION

	YES	NO
14. MEDICAL/FINANCIAL (*"Yes" answers must be explained. Attach additional sheets, if necessary.*)		
a. Have you ever used any narcotic, depressant, stimulant, hallucinogen *(including LSD and PCP)* or cannabis *(including marijuana and hashish)*, except as prescribed by a licensed physician?		
b. Have you ever been involved in the illegal purchase, possession, or sale of any narcotic, depressant, stimulant, hallucinogen, or Cannabis?		
c. Has your use of alcoholic beverages *(such as liquor, beer or wine)* ever resulted in the loss of a job, arrest by police, or treatment for alcoholism or resulted in disciplinary action?		
d. Have you ever had or been treated for a mental, emotional, psychological, or personality disorder/condition/problem?		
e. Have you ever petitioned to be declared bankrupt or experienced other financial difficulties?		

15. ORGANIZATIONS

a. *List all organizations, except labor unions, and those referred to in b. below, to which you belong or previously belonged.*

(1) NAME	(2) ADDRESS	(3) TYPE	(4) FROM	(5) TO

	YES	NO
b. (*"Yes" answers must be explained. Attach additional sheets, if necessary.*)		
(1) Are you now or have you ever been a member of the Communist Party or any Communist organization?		
(2) Are you now or have you ever been affiliated with any organization, association, movement, group, or combination of persons which advocates the overthrow of our constitutional form of government, or which has adopted the policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States or which seeks to alter the form of government of the United States by unconstitutional means?		
16. SECURITY CLEARANCE (*"Yes" answers must be explained. Attach additional sheets, if necessary.*)		
Have you ever had a security clearance denied, revoked, or suspended?		
17. DISCHARGE FROM THE ARMED FORCES (*"Yes" answers must be explained. Attach additional sheets, if necessary.*)		
Have you ever been discharged from the Armed Forces under other than honorable conditions?		

18. **EMPLOYEE CERTIFICATION**

I certify that the entries made by me are true, complete, and accurate to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine, imprisonment, or both. *(See Title 18, U.S. Code, Section 10001)*

a. TYPED OR PRINTED NAME	b. SIGNATURE	c. SOCIAL SECURITY NUMBER	d. DATE SIGNED (YYMMDD)

DD Form 48-3, AUG 87 — Page 2 of 2 Pages

PRIVACY ACT STATEMENT FOR DD FORM 48-3

AUTHORITY: Executive Order 10865, as amended by Executive Order 10909, Safeguarding Information Within Industry; Executive Order 9397, November 1943 (SSN).

PRINCIPAL PURPOSE: To determine the individual's eligibility for an industrial Personnel Security Clearance.

ROUTINE USES: Used by DISCO to establish and maintain records of Industrial Personnel Security Clearance actions. The Social Security Number is used as the primary identifying factor in the system of records. Access to or use of the personal information furnished is generally limited to authorized Federal Government employees, law enforcement and investigative agencies for official personnel security investigative and clearance functions and to authorized contractor personnel performing clearance processing duties. Interim notification to contractor personnel that a security clearance has been issued may be transmitted over a Government or Commercial telecommunications network. This interim notification will include the individual's name and Social Security Number and the level and date of the security clearance. Contractor access to privacy portions of all Personnel Security Questionnaires remains prohibited. In the case of a Canadian or United Kingdom reciprocal personnel security clearance, or security assurance required by any other foreign government, minimal information will be provided, as required.

DISCLOSURE: Voluntary, however, if the requested information is not provided, further processing for a personnel security clearance will be discontinued or action initiated to withdraw any clearance presently in existence.

Detached from DD Form 48-3, AUG 87

*U.S.GPO:1987-0-748-128/60825

F. "Department of Defense Personnel Security Questionnaire (Industrial)" (DD Form 49). This form shall be used in making application for:

1. a U.S. citizen being considered for a TOP SECRET PCL,

2. a U.S. citizen being considered for any level of clearance, when the individual advises that he or she is an RFI,

3. a U.S. citizen who has relatives or relatives of his or her spouse who are residing in Designated countries,

4. an immigrant alien being considered for an LAA, and

5. a citizen of a signatory country being processed for an LAA.

The form is prepared jointly by management and the person being considered for clearance. The completed form shall be forwarded to DISCO, P.O. Box 2499, Columbus, Ohio 43216-5006. Forms that pertain to OODEPs, which are submitted in conjunction with the FCL application, shall be appropriately marked "OODEP" in item e (To be Completed by Employer) in lieu of the contract number. * * *

SAMPLE
DD Form 49

SECTION I
PERSONNEL SECURITY QUESTIONNAIRE
INDUSTRIAL
DD FORM 49

Public reporting burden for this collection of information is estimated to average 1.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0002), Washington, DC 20503.

Privacy Act Statement

AUTHORITY: Internal Security Act of 1950, EO 10865, as amended by EO 10909, and EO 9397, November 1943 (SSN).

PRINCIPAL PURPOSES: To obtain background information for personnel security investigative and evaluative purposes in order to determine the security eligibility of Department of Defense contractors and employees of Department of Defense contractors for (1) access to classified information, or (2) assignment to a sensitive position.

ROUTINE USES: (1) Determine the scope of a personnel security investigation.

(2) Provide evaluators or adjudicators with personal history information relevant to personnel security determinations.

The information may be disclosed to other Federal agencies that are authorized under specific statutory or Executive authority to make personnel security determinations.

A copy of the report of personnel security investigation will be maintained by the Personnel Investigations Center of the Defense Investigative Service and may be used in future security clearance determinations. You have the right to obtain a copy of the report of investigation and/or request amendment to the file.

DISCLOSURE: Voluntary. Failure, however, to furnish all or part of the information requested may result in (1) denial of access to classified information, or (2) non-selection for assignment to a sensitive position. Disclosure of your Social Security Number is necessary to fulfill requirements of the above cited authorities. It is intended that this notice be retained for personal records.

GENERAL INSTRUCTIONS

THE ATTACHED PACKET OF MATERIAL CONSISTS OF **TWO SECTIONS:** SECTION **I–A DD FORM 49 WORKSHEET PRINTED ON THE REVERSE OF THESE INSTRUCTIONS** AND THE DD FORM 49 PACKAGED AS A 5-COPY CARBON INTERLEAF SET; SECTION II – A DD FORM 2221 AND AN ORIGINAL AND ONE COPY OF THE PRIVACY SECTION. DETACH THE WORKSHEET AND COMPLETE ITEMS 1-16. WHEN YOU ARE SATISFIED THAT ALL ITEMS ARE CORRECT AND COMPLETE IN ACCORDANCE WITH THE DETAILED INSTRUCTIONS WHICH YOU HAVE BEEN FURNISHED, TURN THE WORKSHEET OVER TO YOUR EMPLOYER WHO WILL REVIEW IT TO ASSURE THAT ALL ENTRIES ARE COMPLETE AND ACCURATE. AT THIS POINT ENTER THE ENTRIES FROM THE WORKSHEET ONTO THE DD FORM 49 5-COPY CARBON INTERLEAF SET USING A BALL-POINT PEN OR TYPEWRITER (YOUR EMPLOYER MAY HAVE THE FORM TYPED FOR YOU). BE SURE YOU SIGN THE FORM AT THE BOTTOM UNDER THE REMARKS SECTION. WHEN THE DD FORM 49 HAS BEEN COMPLETED AND SIGNED, COMPLETE SECTION II – THE PRIVACY SECTION TO INCLUDE ENTRY OF YOUR SIGNATURE, AND THEN SIGN AND DATE THE DD FORM 2221. PLACE ALL COMPLETED MATERIAL, TOGETHER WITH A COMPLETED FD FORM 258 (FINGERPRINT CARD) IN THE PRE-ADDRESSED ENVELOPE THAT HAS BEEN PROVIDED. SEAL THE ENVELOPE, SIGN ACROSS THE ENVELOPE FLAP ON THE LINE PROVIDED AND AFFIX THE DATE OF SIGNATURE. DELIVER THE SEALED ENVELOPE TO YOUR EMPLOYER IMMEDIATELY. IN COMPLETING THE PACKET OF MATERIAL, THE FOLLOWING APPLY:

- THE PERSONNEL SECURITY QUESTIONNAIRE (PSQ) IS AN IMPORTANT DOCUMENT AND MUST BE COMPLETED WITHOUT MISSTATEMENT OR OMISSION OF IMPORTANT FACTS. ALL ENTRIES ARE SUBJECT TO VERIFICATION BY INVESTIGATION.
- ENTRIES MUST BE TYPED OR PRINTED.
- IF ADDITIONAL SPACE IS REQUIRED FOR ANY ITEM, USE ITEM 16, "REMARKS." IF SPACE PROVIDED IN ITEM 16 IS INSUFFICIENT, USE SEPARATE SHEET(S) OF PLAIN WHITE PAPER. WHEN ATTACHING ADDITIONAL SHEETS ALWAYS IDENTIFY THE ITEM NUMBER BEING CONTINUED AND FOLLOW THE FORMAT FOR ENTERING INFORMATION PRESCRIBED ON THE FORM AND IN THE DETAILED INSTRUCTIONS.
- ALL QUESTIONS MUST BE ANSWERED. IF AN ITEM IS NOT APPLICABLE INDICATE "NOT APPLICABLE." OR "N/A." DO NOT USE THE TERM "UNKNOWN" FOR DATE OF EMPLOYMENT OR RESIDENCE. IF THIS INFORMATION IS NOT KNOWN PRECISELY, GIVE THE DATE AS BEST YOU CAN RECALL FOLLOWED BY APPROPRIATE QUALIFYING LANGUAGE, E.G., "DATE ESTIMATED" OR "APPROX."
- UNLESS OTHERWISE SPECIFIED:
  - ALL DATES SHOULD BE ENTERED IN TERMS OF YEAR AND MONTH USING THE LAST TWO DIGITS OF THE YEAR AND A TWO DIGIT NUMBER REPRESENTING THE MONTH, E.G., JANUARY 1979 WOULD BE ENTERED AS 79-01 AND DECEMBER 1979 WOULD BE ENTERED AS 79-12.
  - NAMES OF PERSONS SHOULD BE ENTERED IN THE FOLLOWING ORDER: LAST NAME, FIRST NAME AND MIDDLE INITIAL.
  - ADDRESSES SHOULD INCLUDE THE NUMBER AND STREET, CITY, STATE OR COUNTRY, AND ZIP CODE.
- BEFORE ENTERING ANY INFORMATION, READ CAREFULLY THE DETAILED INSTRUCTIONS PROVIDED WITH THE PACKET. IF AT ANY TIME DURING COMPLETION OF THE MATERIAL, A QUESTION ARISES THAT DOES NOT APPEAR TO BE COVERED BY THE DETAILED INSTRUCTIONS, CONTACT THE INDIVIDUAL OR OFFICE THAT PROVIDED YOU WITH THE MATERIAL.

DD Form 49 Instructions, JAN 89

SAMPLE
DD Form 49
Page Two

DEPARTMENT OF DEFENSE
PERSONNEL SECURITY QUESTIONNAIRE *(INDUSTRIAL)*

Form Approved
OMB No. 0704-0002
Expires Apr 30, 1991

DATE

FOR DIS USE ONLY

1. a. LAST NAME – FIRST NAME – MIDDLE NAME
b. MAIDEN NAME *(If any)*

2. ALIASES

3. a. SEX ☐ Male ☐ Female

b. RACE

4. SOCIAL SECURITY NUMBER

5. DATE OF BIRTH *(Yr - Mo - Day)*

6. PLACE OF BIRTH a. CITY b. COUNTY c. STATE d. COUNTRY

7.a. U.S. CITIZEN ☐ Yes ☐ No
b. NATIVE ☐ Yes ☐ No
c. IF NATURALIZED, CERTIFICATE NO.(s)
d. IF DERIVED, PARENT(s) CERTIFICATE NO.(s)
e. DATE
f. PLACE
g. COURT
h. DUAL CITIZEN ☐ Yes ☐ No *(If "Yes," see DETAILED INSTRUCTIONS.)*

8. MILITARY SERVICE *(Include Reserve/National Guard)*

a. FROM	b. TO	c. BRANCH	d. RANK	e. SERVICE NO(S).	f. COUNTRY

9. PREVIOUS CLEARANCE LEVEL

	Yes	No
a. HAVE YOU EVER APPLIED FOR A SECURITY CLEARANCE? *(If "Yes," give details below.)*		

(1) Level	(2) Date Granted	(3) Granted By	(4) Name of Employer

	Yes	No
b. Have you ever terminated employment while request for security clearance was pending? *("Yes" answer must be explained in accordance with the DETAILED INSTRUCTIONS.)*		

10. FAMILY / ASSOCIATES *(See DETAILED INSTRUCTIONS for persons to be listed.)*

a. RELATIONSHIP AND NAME	b. DATE OF BIRTH	c. PLACE OF BIRTH	d. ADDRESS	e. CITIZENSHIP
Father				
Mother *(Maiden Name)*				
Spouse *(Maiden Name)*				
Former Spouse				

11. RESIDENCES *(Begin with current address - see DETAILED INSTRUCTIONS.)*

a. DATES (Yr & Mo)		b. NUMBER AND STREET	c. CITY	d. STATE	e. ZIP CODE
From	To				
	Present				

12. EMPLOYMENT *(Include self-employment, part-time employment and / or unemployment. See DETAILED INSTRUCTIONS.)*

a. DATES *(Yr & Mo)*		b. NAME OF EMPLOYER	c. ADDRESS	d. ZIP CODE	e. SUPERVISOR
From	To				
	Present				

13. FEDERAL SERVICE, FOREIGN TRAVEL / CONNECTIONS *(If "Yes," see DETAILED INSTRUCTIONS.)*	Yes	No
a. Have you ever been in the Federal Civil Service?		
b. Have you traveled or resided abroad for other than the U.S. Government?		
c. Do you have any foreign property or business connections or have you ever been employed by or acted as a consultant or representative for a foreign government, firm, or agency?		

TO BE COMPLETED BY EMPLOYER a. LEVEL OF CLEARANCE ☐ Top Secret ☐ SCI ☐ Other *(Specify)*

b. CITIZENSHIP VERIFIED ☐ Yes ☐ No
c. JOB TITLE
d. FEDERAL SUPPLY CODE
e. CONTRACT NUMBER

f. CERTIFICATION - I certify that the above named individual is employed by this company and has the need for the clearance indicated to perform on classified contracts.

DATE
SIGNATURE OF EMPLOYER OR DESIGNATED REPRESENTATIVE

DD Form 49, JAN 89 *Previous editions are obsolete.*

SAMPLE
DD Form 49
Page Three

14. EDUCATION *(Begin with last school attended - see DETAILED INSTRUCTIONS.)*

a. DATES (Yr & Mo)		b. NAME OF SCHOOL	c. ADDRESS	d. ZIP CODE	e. DEGREE
From	To				

15. CHARACTER REFERENCES *(List 5 good friends, co-workers, etc. - see DETAILED INSTRUCTIONS.)*

a. NAME	b. PERIOD KNOWN	c. ADDRESS	d. TELEPHONE

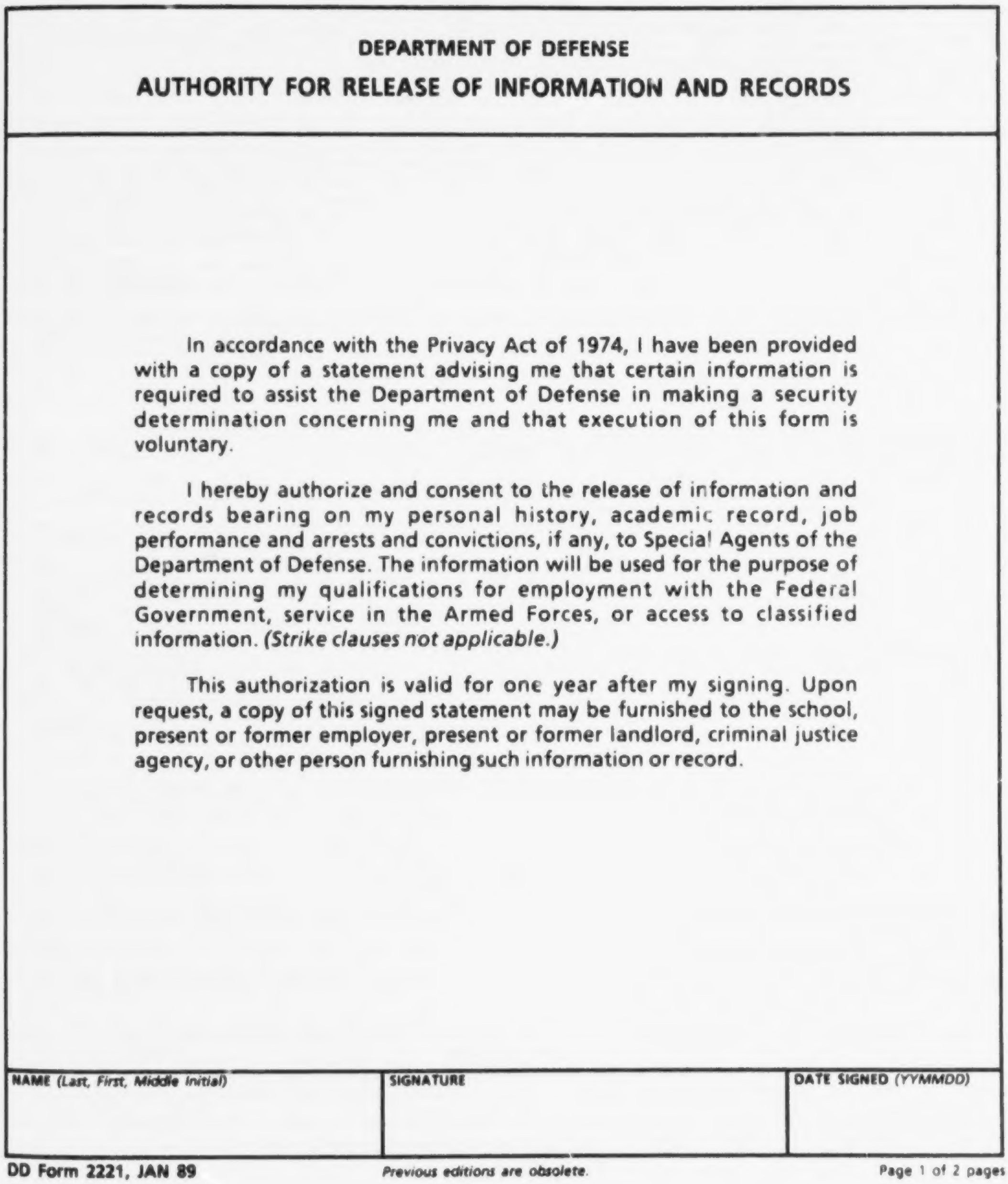
16. REMARKS *(Attach additional sheets, if necessary.)*

DATE	SIGNATURE OF PERSON COMPLETING FORM

DD Form 49 Reverse, JAN 89

SAMPLE
DD Form 49
Page Four

SECTION II OF DD FORM 49



DEPARTMENT OF DEFENSE

AUTHORITY FOR RELEASE OF INFORMATION AND RECORDS

In accordance with the Privacy Act of 1974, I have been provided with a copy of a statement advising me that certain information is required to assist the Department of Defense in making a security determination concerning me and that execution of this form is voluntary.

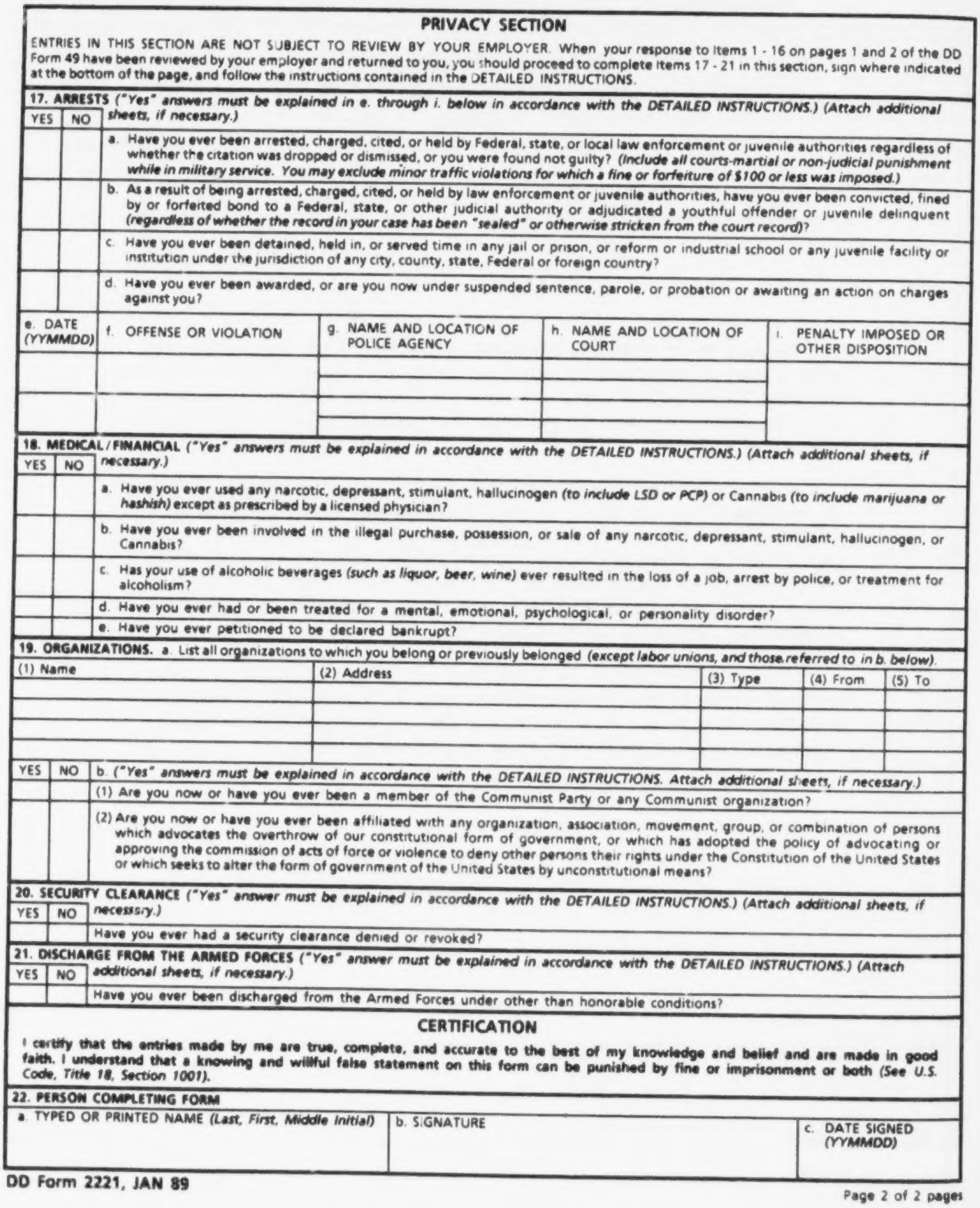
I hereby authorize and consent to the release of information and records bearing on my personal history, academic record, job performance and arrests and convictions, if any, to Special Agents of the Department of Defense. The information will be used for the purpose of determining my qualifications for employment with the Federal Government, service in the Armed Forces, or access to classified information. *(Strike clauses not applicable.)*

This authorization is valid for one year after my signing. Upon request, a copy of this signed statement may be furnished to the school, present or former employer, present or former landlord, criminal justice agency, or other person furnishing such information or record.

NAME *(Last, First, Middle Initial)*	SIGNATURE	DATE SIGNED *(YYMMDD)*

DD Form 2221, JAN 89 *Previous editions are obsolete.* Page 1 of 2 pages

SAMPLE
DD Form 49
Page Five



PRIVACY SECTION

ENTRIES IN THIS SECTION ARE NOT SUBJECT TO REVIEW BY YOUR EMPLOYER. When your response to Items 1 - 16 on pages 1 and 2 of the DD Form 49 have been reviewed by your employer and returned to you, you should proceed to complete Items 17 - 21 in this section, sign where indicated at the bottom of the page, and follow the instructions contained in the DETAILED INSTRUCTIONS.

17. ARRESTS *("Yes" answers must be explained in e. through i. below in accordance with the DETAILED INSTRUCTIONS.) (Attach additional sheets, if necessary.)*

YES	NO	
		a. Have you ever been arrested, charged, cited, or held by Federal, state, or local law enforcement or juvenile authorities regardless of whether the citation was dropped or dismissed, or you were found not guilty? *(Include all courts-martial or non-judicial punishment while in military service. You may exclude minor traffic violations for which a fine or forfeiture of $100 or less was imposed.)*
		b. As a result of being arrested, charged, cited, or held by law enforcement or juvenile authorities, have you ever been convicted, fined by or forfeited bond to a Federal, state, or other judicial authority or adjudicated a youthful offender or juvenile delinquent *(regardless of whether the record in your case has been "sealed" or otherwise stricken from the court record)*?
		c. Have you ever been detained, held in, or served time in any jail or prison, or reform or industrial school or any juvenile facility or institution under the jurisdiction of any city, county, state, Federal or foreign country?
		d. Have you ever been awarded, or are you now under suspended sentence, parole, or probation or awaiting an action on charges against you?

e. DATE *(YYMMDD)*	f. OFFENSE OR VIOLATION	g. NAME AND LOCATION OF POLICE AGENCY	h. NAME AND LOCATION OF COURT	i. PENALTY IMPOSED OR OTHER DISPOSITION

18. MEDICAL/FINANCIAL *("Yes" answers must be explained in accordance with the DETAILED INSTRUCTIONS.) (Attach additional sheets, if necessary.)*

YES	NO	
		a. Have you ever used any narcotic, depressant, stimulant, hallucinogen *(to include LSD or PCP)* or Cannabis *(to include marijuana or hashish)* except as prescribed by a licensed physician?
		b. Have you ever been involved in the illegal purchase, possession, or sale of any narcotic, depressant, stimulant, hallucinogen, or Cannabis?
		c. Has your use of alcoholic beverages *(such as liquor, beer, wine)* ever resulted in the loss of a job, arrest by police, or treatment for alcoholism?
		d. Have you ever had or been treated for a mental, emotional, psychological, or personality disorder?
		e. Have you ever petitioned to be declared bankrupt?

19. ORGANIZATIONS. a. List all organizations to which you belong or previously belonged *(except labor unions, and those referred to in b. below)*.

(1) Name	(2) Address	(3) Type	(4) From	(5) To

YES	NO	b. *("Yes" answers must be explained in accordance with the DETAILED INSTRUCTIONS. Attach additional sheets, if necessary.)*
		(1) Are you now or have you ever been a member of the Communist Party or any Communist organization?
		(2) Are you now or have you ever been affiliated with any organization, association, movement, group, or combination of persons which advocates the overthrow of our constitutional form of government, or which has adopted the policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States or which seeks to alter the form of government of the United States by unconstitutional means?

20. SECURITY CLEARANCE *("Yes" answer must be explained in accordance with the DETAILED INSTRUCTIONS.) (Attach additional sheets, if necessary.)*

YES	NO	
		Have you ever had a security clearance denied or revoked?

21. DISCHARGE FROM THE ARMED FORCES *("Yes" answer must be explained in accordance with the DETAILED INSTRUCTIONS.) (Attach additional sheets, if necessary.)*

YES	NO	
		Have you ever been discharged from the Armed Forces under other than honorable conditions?

CERTIFICATION

I certify that the entries made by me are true, complete, and accurate to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (See U.S. Code, Title 18, Section 1001).

22. PERSON COMPLETING FORM

a. TYPED OR PRINTED NAME *(Last, First, Middle Initial)*	b. SIGNATURE	c. DATE SIGNED *(YYMMDD)*

DD Form 2221, JAN 89

Page 2 of 2 pages

G. "Department of Defense Contract Security Classification Specification" (DD Form 254).

1. The completed DD Form 254, with attachments and supplements, as applicable, is the basic document by which classification, regrading, and declassification specifications are documented and provided to prime contractors and subcontractors. It is designed to identify the specific items of classified information involved in the contract that require security classification protection. Responsibility for preparation of the prime contract's DD Form 254 rests with the contracting officer or the designated representative of the UA concerned, but the assistance of the contractor is encouraged. Based on the classification guidance received, each contractor is responsible for developing the DD Form 254 for each classified subcontract, request for proposal, or other solicitation let to subcontractor facilities. The contractor shall submit the recommended DD Forms 254 for each classified subcontract, other than service, graphic arts, or commercial carrier subcontracts (see paragraph 60h) to the ACO for approval and distribution. When the prime contractor receives a revised DD Form 254 that does not require a related change in the subcontractor's DD Form 254, or receives written notice that the biennial review has resulted in no change in the existing specification, he or she shall reaffirm guidance to each subcontractor. The prime contractor does this by providing a true copy of the notice of reaffirmation received by the prime contractor or a true copy of pages 1 and 2 of the revised DD Form 254 received by the prime contractor annotated, "This revised DD Form 254 does not affect your current DD Form 254 dated ______________." In either of these cases, ACO/PCO authentication is not required.

2. The DD Form 254 embodies the concept that the sensitive information itself shall be identified and assigned a proper classification, rather than assigning a classification to media by which classified information could be, or would likely be, conveyed. This method of classifying information rather than media is intended to identify most precisely the functional matter that is to be protected; thus providing, for example, the answer to the question: "What is there about a specific item of hardware which causes it to be classified?"

3. Whenever the prime contractor will be required to use classified GFE or GFP in the performance of the contract, the contracting officer or the designated representative shall inform the prime contractor what information requires protection by furnishing a DD Form 254 or other appropriate notification for each item of classified GFE or GFP to be used. The same procedure shall be followed in those instances where previously classified equipment is not government-furnished and the prime contractor is authorized to purchase such classified equipment for use in the performance of his or her contract.

4. Items 1 through 14 and item 16 of the DD Form 254 provide the general administrative and contractual information pertaining to the classification specification of the classified effort. Item 15 of DD Form 254, with any supplements and attachments, is used to provide the specified classification downgrading and declassification information. Each item of the DD Form 254 is to be completed; N/A shall be shown for items that are not applicable.

Classified information should not be entered on the DD Form 254. Classified information should be transmitted separately and appropriate references entered in item 15 of the DD Form 254. The following numbered instructions correspond to the numbered items on the DD Form 254.

a. Item 1. Insert highest level of clearance required for access to classified effort. If the facility requires a clearance higher than the current clearance, the prime contractor may request the appropriate CSO to upgrade the subcontractor's FCL.

b. Item 2. Check item a, b, or c, as applicable.

c. Item 3. In item 3a, enter the UA prime contract identification number. In addition, if this DD Form 254 is for a subcontract of the first tier, enter in item 3b the identification number of the first tier subcontract. For second tier and beyond subcontracts, enter in item 9a or 15, as applicable, the identification number, and estimated date of completion or termination of the subcontract. If item 3c is used, enter appropriate data identifying the RFP, RFQ, or IFB. If the solicitation is unclassified and the DD Form 254 is being used only to reflect access requirements of the contract/subcontract to be awarded, annotate item 11o "Remarks" to indicate that preaward access is not required and the DD Form 254 indicates classification guidance for the contract/subcontract to be awarded. When reissuing a currently valid subcontract DD Form 254 for a follow-on subcontract, indicate the new subcontract number in item 3b.

d. Item 4. Furnish date for a, b, or c, as applicable.

e. Item 5. Check item a, b, or c, as applicable, and provide complete data. For item b, also show revision number.

f. Item 6. Check "yes" or "no", as applicable. If "yes," complete items a and b, and in item c, indicate whether accountability is or is not transferred.

g. Item 7. If there is a prime contract, complete items a, b, and c, to show the complete name, address, FSC number, and the CSO of the prime contractor's facility that will receive classified information in the performance of the prime contract listed in item 3a. If there is no prime contract and item 3c is completed, enter instead in items a, b, and c, the name, address, and FSC number of the contractor's facility to which this DD Form 254 is to be sent in connection with the RFP, RFQ, or IFB, and the CSO of that facility.

h. Item 8. If there is a first tier subcontract, complete items a, b, and c, to show the complete name, address, and FSC number of the subcontractor's facility that will receive classified information in the performance of the subcontract listed in item 3b. If there is no first tier subcontract and item 3c is completed, enter instead the name, address, and FSC number of the subcontractor's facility to which this DD Form 254 is to be sent in connection with the RFP, RFQ, or IFB, and CSO of that facility.

i. Item 9. If there is a second tier subcontract, complete items a, b, and c to show the complete name, address, FSC number, and CSO of the subcontractor's facility that will receive classified information in performance of the subcontract listed in item 3b. In item 9a, also provide the second tier subcontract number and estimated date of completion. If there is no second tier subcontract and item 3c is completed, enter instead the name, address, FSC number, and the CSO of the facility to which this DD Form 254 is to be sent in connection with the RFP, RFQ, or IFB. For subcontracting beyond the second tier, enter in item 15, or furnish on an attached sheet, the information specified above for that tier subcontractor and the CSO of that facility.

j. Item 10. Under item a, provide a brief, yet sufficiently complete, unclassified statement to identify the nature of the procurement. If an unclassified statement cannot be made, enter the word "classified." Under item b, furnish the DoD AAD number of the U.S. Government procuring activity (identified in item 16d). For all subcontractors and first and second tier RFPs, RFQs, and IFBs enter "N/A." Under item c, check appropriate block to indicate whether or not contract prescribes security requirements that are additional to those described in the DD Form 441 and this manual. If applicable, the UA shall furnish a copy of the special security requirements to the contractor, the ACO, if any, and the CSO. Under item d, check appropriate box to indicate if any elements of the contract are outside the inspection responsibility of the CSO. If "Yes," explain in item 15 and identify specific areas or elements. However, discretion must be used in identifying other "specific areas or elements," so that disclosure restrictions are respected.

k. Item 11. Check appropriate box for each item listed. Use the "Remarks" block to elaborate as necessary 1/. If DTIC or Defense Information Analysis Center services are requested, the DD Form 1540 and DD Form 1541 should be prepared and processed, in accordance with component implementations of DoD Instruction 5200.21. Whenever possible, the DD Form 1540 should be prepared and forwarded simultaneously with the DD Form 254.

l. Item 12. In subcontracting situations, item b will contain the signature and typed name and title of the FSO or the designated representative issuing the subcontract. Inquiries pertaining to classification guidance, determinations, or interpretations shall be directed to this official.

m. Item 13. Subcontractors of all tiers shall be instructed, via item b, to submit proposed public releases through the prime contractor listed in item 7a who will then process the release in accordance with the guidance provided in the DD Form 254 for the prime contract.

1/ The entry into a controlled area, per se, will not constitute access to classified information, if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a PCL.

n. Item 14. Read and closely observe the instructions presented at the top half of the item. Check applicable block(s) to indicate the manner in which the security classification guidance is conveyed for this classified effort. Classified narratives or guides shall always be transmitted under separate cover. When item b is checked, list guide(s) under item 15 or in an attached list. When item c is checked, enter in item 15 the appropriate instructions from paragraph 60h. (See paragraph 5 below for an explanation of commonly used terms.) Check item d if this is a final DD Form 254 and item 6 has a "No" answer. Check item e and provide date for review when biennial review of DD Form 254 is required.

o. Item 15. Should be used for remarks, as appropriate.

p. Item 16. The contracting officer or authorized designee, after reviewing the DD Form 254 to ensure adequacy, will affix his or her signature in item c, and items b, d, and e, will be completed to furnish appropriate identifying information concerning the approving official.

5. Narratives or classification guides used to provide the security classification specifications and the downgrading and declassification instructions should clearly identify the specific details of information that warrant security protection against unauthorized disclosure. It is important to ensure that statements of classification are clear enough to be easily understood and applied readily in determining which items of information in the contractual effort require a security classification. To assist the writer and user of the security classification specification, there are listed below several terms, which are commonly used in the description of that information which may require classification, together with their generally accepted meanings. However, this does not preclude inclusion of terms devoted to a particular classified effort or an additional page(s) of the narrative/guide.

a. Accuracy. This refers to the precision with which the designed function is performed.

b. Altitude. The vertical distance of a level, a point, or an object considered as a point that is measured from mean sea level is the altitude.

(1) Maximum. This is the altitude beyond which performance is not possible.

(2) Minimum. This is the altitude below which performance is not possible.

(3) Optimum. This is the altitude spread at which performance is most satisfactory or effective.

c. Blast Effect. This refers to the destruction of, or damage to, structures and personnel by the force of an explosion on or above the surface of the ground. Blast effect may be contrasted with the cratering and ground shock effects of a projectile or charge that goes off beneath the surface.

d. Circular Error Probability. An indicator of the delivery accuracy of a weapon system that is used as a factor in determining probable damage to a target is the circular error probability. It is the radius of a circle within which half of the missiles/projectiles are expected to fall.

e. Command and Control System. This refers to the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.

f. Counter-Countermeasures Capability. Design features of the end item that are intended specifically to overcome enemy interference make up the counter-countermeasures capability. (Electronic counter-countermeasures is that division of electronic warfare involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of electronic warfare. Electronic countermeasures is that division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum.)

g. Depth. Depth is the vertical distance from the plane of the hydrographic surface to a level, a point, or an object considered as a point below the surface.

(1) Maximum. This is the depth below which performance is not possible.

(2) Minimum. This is the depth above which performance is not possible.

(3) Optimum. This is the depth spread at which performance is most satisfactory or effective.

h. Design Information. This refers to a technique, principle, or design feature, or the unique application thereof, which in and of itself requires classification. The design information that requires protection must be specified.

i. End Item. This refers to a final combination of end products, component parts, and/or materials that is ready for its intended use, for example, ships, tanks, mobile machine shops, and aircraft.

j. Endurance. Endurance is the time an aircraft can continue flying or a ground vehicle or ship can continue operating under specified conditions, for example, without refueling.

k. Formula or Material. The chemical or physical nature of the ingredient(s) and its proportions make up a formula or material of which all, or part of, the end item is composed.

l. Fuel or Propellant. Source of energy. Type. Identification of fuel/propellant.

m. Initial Operational Capability. This is the first attainment of the capability to employ effectively a weapon, item of equipment, or system of approved specific characteristics, which is manned or operated by an adequately trained, equipped, and supported military unit or force.

n. Lethality/Critical Effects. The ability to cause a specified degree of damage to the target or to incapacitate personnel (including physical, physiological, and psychological effects) is described as lethality/critical effects.

o. Maneuverability. This is the ability to change position or direction.

p. Military Application. The military application is the use or purpose for which the end item is intended in sufficient detail that performance and/or tactical application is revealed or implied.

q. Military Characteristics. Those characteristics of equipment which reflect its ability to perform desired military functions are military characteristics. Military characteristics include physical and operational characteristics, but not technical characteristics.

r. Mission. A mission is the task, together with the purpose, which clearly indicates the action to be taken and the reason therefor.

s. Operational Characteristics. Those military characteristics which pertain primarily to the functions to be performed by equipment, either alone or in conjunction with other equipment, are operational characteristics. For example, for electronic equipment, operational characteristics include such items as frequency coverage, channeling, type of modulation, and character of emission.

t. Operational Readiness (Alert) Time/Time Cycle. This refers to the sequence and duration of important operations to be performed on or by the end items or specified component thereof during a normal cycle of function such as emplacement, loading and firing/launching, and warm-up prior to operation.

u. Orbit/Trajectory. The path of travel is the orbit/trajectory.

v. Range. The distance between any given point and an object or target is the range. This also refers to the extent or distance limiting the operation or action of something, such as the range of an aircraft, ship, or gun.

(1) Maximum. This is the greatest distance attainable.

(2) Minimum. This is the shortest distance attainable or allowable.

(3) Optimum. This is the range spread at which performance is most satisfactory or effective.

w. Reliability. This is the probability that the design function will be performed at or for a specified time and/or within specified limits.

x. Resolutions. This refers to the ability to analyze characteristics of a complex nature (such as signals and target signature characteristics) and to distinguish between them.

y. Signature Characteristics. Acoustic, magnetic, thermal, radiological, mechanical, electromagnetic, and similar phenomena that are critical to the operation of the end item or a component thereof, or that identify or reveal its presence are signature characteristics.

z. Speed/Velocity. This is the rate of movement or motion.

(1) Maximum. This is the greatest speed/velocity attainable.

(2) Cruising. This is the speed/velocity at which greatest efficiency is attained.

(3) Take-off or Launching. This is the speed/velocity needed to initiate flight.

(4) Landing. This is the speed/velocity needed in terminating flight.

(5) Acceleration and/or Deceleration. This is the rate of change of speed/velocity.

aa. System Capability. This refers to the maximum number of operations that the end item can perform simultaneously in carrying out its design function.

ab. Technical Characteristics. Those characteristics of equipment that pertain primarily to the engineering principles involved in producing equipment possessing desired military characteristics are technical characteristics. For example, for electronic equipment, technical characteristics include such items as circuitry and types and arrangement of components.

ac. Terminal Ballistics. Terminal ballistics are the effects and actions of a missile or projectile when it impacts or bursts at the target.

ad. Thrust. Thrust refers to the impelling force delivered.

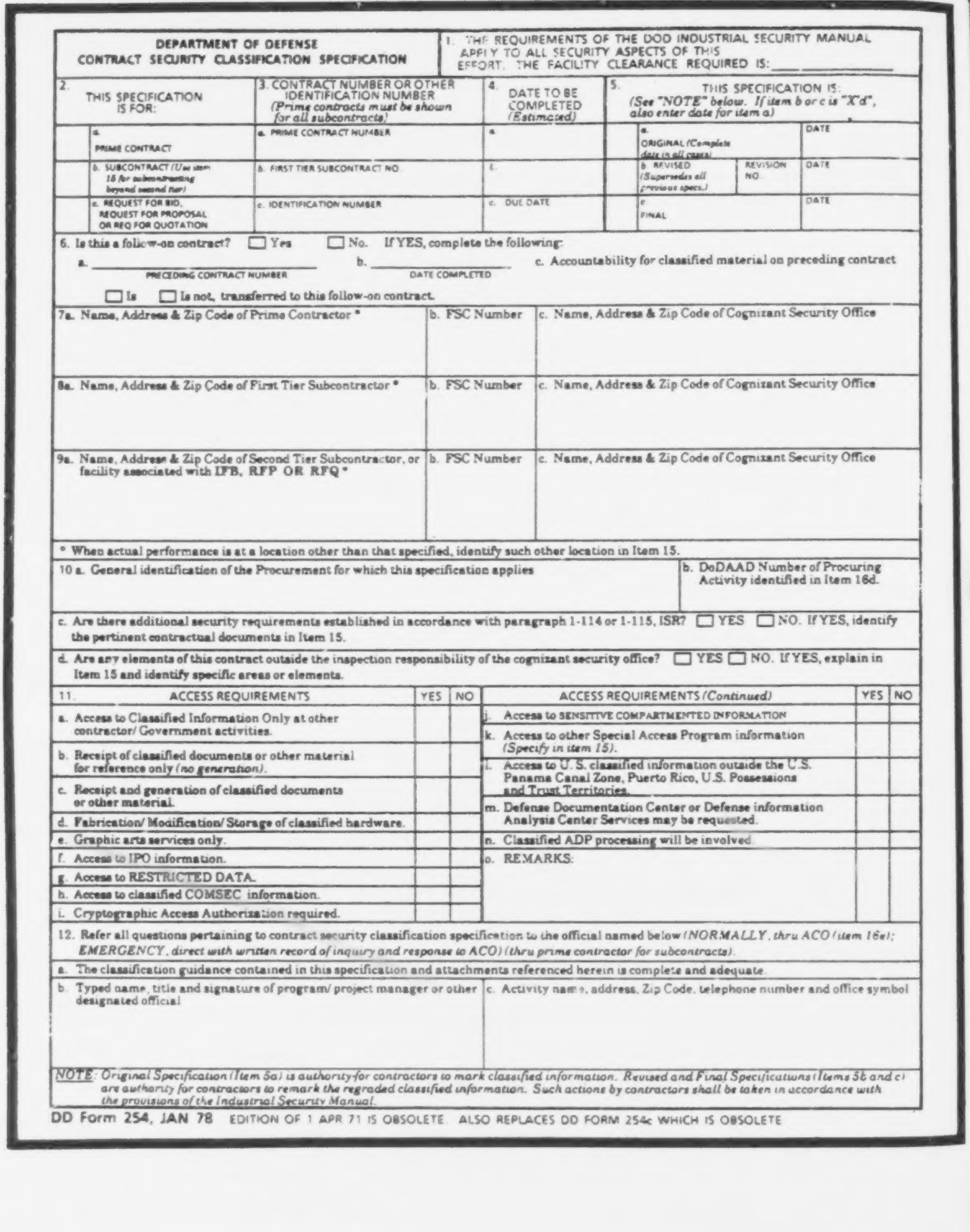
(1) Classes -- maximum thrust expressed as an approximation or within a grouping

(2) Specific -- exact maximum thrust

(3) Specific Impulse -- amount of thrust in pounds that can be maintained for one second by one pound of fuel

ae. Vulnerability. Vulnerability refers to the susceptibility to defeat by the enemy.

SAMPLE
DD Form 254



DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

1. THE REQUIREMENTS OF THE DOD INDUSTRIAL SECURITY MANUAL APPLY TO ALL SECURITY ASPECTS OF THIS EFFORT. THE FACILITY CLEARANCE REQUIRED IS: ____________

2. THIS SPECIFICATION IS FOR:	3. CONTRACT NUMBER OR OTHER IDENTIFICATION NUMBER *(Prime contracts must be shown for all subcontracts)*	4. DATE TO BE COMPLETED *(Estimated)*	5. THIS SPECIFICATION IS: *(See "NOTE" below. If item b or c is "X'd", also enter date for item a)*		
a. PRIME CONTRACT	a. PRIME CONTRACT NUMBER	a.	a. ORIGINAL *(Complete date in all cases)*		DATE
b. SUBCONTRACT *(Use item 18 for subcontracting beyond second tier)*	b. FIRST TIER SUBCONTRACT NO.	b.	b. REVISED *(Supersedes all previous specs.)*	REVISION NO.	DATE
c. REQUEST FOR BID, REQUEST FOR PROPOSAL OR REQ FOR QUOTATION	c. IDENTIFICATION NUMBER	c. DUE DATE	c. FINAL		DATE

6. Is this a follow-on contract? ☐ Yes ☐ No. If YES, complete the following:
a. ____________ PRECEDING CONTRACT NUMBER
b. ____________ DATE COMPLETED
c. Accountability for classified material on preceding contract ☐ Is ☐ Is not, transferred to this follow-on contract.

7a. Name, Address & Zip Code of Prime Contractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
8a. Name, Address & Zip Code of First Tier Subcontractor *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office
9a. Name, Address & Zip Code of Second Tier Subcontractor, or facility associated with IFB, RFP OR RFQ *	b. FSC Number	c. Name, Address & Zip Code of Cognizant Security Office

* When actual performance is at a location other than that specified, identify such other location in Item 15.

10 a. General identification of the Procurement for which this specification applies

b. DoDAAD Number of Procuring Activity identified in Item 16d.

c. Are there additional security requirements established in accordance with paragraph 1-114 or 1-115, ISR? ☐ YES ☐ NO. If YES, identify the pertinent contractual documents in Item 15.

d. Are any elements of this contract outside the inspection responsibility of the cognizant security office? ☐ YES ☐ NO. If YES, explain in Item 15 and identify specific areas or elements.

11. ACCESS REQUIREMENTS	YES	NO	ACCESS REQUIREMENTS *(Continued)*	YES	NO
a. Access to Classified Information Only at other contractor/ Government activities.			j. Access to SENSITIVE COMPARTMENTED INFORMATION		
b. Receipt of classified documents or other material for reference only *(no generation)*.			k. Access to other Special Access Program information *(Specify in item 15)*.		
c. Receipt and generation of classified documents or other material.			l. Access to U. S. classified information outside the U.S. Panama Canal Zone, Puerto Rico, U.S. Possessions and Trust Territories.		
d. Fabrication/ Modification/ Storage of classified hardware.			m. Defense Documentation Center or Defense information Analysis Center Services may be requested.		
e. Graphic arts services only.			n. Classified ADP processing will be involved.		
f. Access to IPO information.			o. REMARKS:		
g. Access to RESTRICTED DATA.					
h. Access to classified COMSEC information.					
i. Cryptographic Access Authorization required.					

12. Refer all questions pertaining to contract security classification specification to the official named below *(NORMALLY, thru ACO (item 16e); EMERGENCY, direct with written record of inquiry and response to ACO) (thru prime contractor for subcontracts)*.

a. The classification guidance contained in this specification and attachments referenced herein is complete and adequate.

b. Typed name, title and signature of program/ project manager or other designated official

c. Activity name, address, Zip Code, telephone number and office symbol

NOTE: Original Specification (Item 5a) is authority for contractors to mark classified information. Revised and Final Specifications (Items 5b and c) are authority for contractors to remark the regraded classified information. Such actions by contractors shall be taken in accordance with the provisions of the Industrial Security Manual.

DD Form 254, JAN 78 EDITION OF 1 APR 71 IS OBSOLETE. ALSO REPLACES DD FORM 254c WHICH IS OBSOLETE

SAMPLE
DD Form 254
Page Two

13 a. Information pertaining to classified contracts or projects, even though such information is considered unclassified, shall not be released for public dissemination except as provided by the Industrial Security Manual *(paragraph 5o and Appendix IX)*.

b. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☐ Through *(Specify)*:

to the Directorate For Freedom of Information and Security Review, Office of the Assistant Secretary of Defense *(Public Affairs)* * for review in accordance with paragraph 5o of the Industrial Security Manual.

** In the case of non-DoD User Agencies, see footnote, paragraph 5o, Industrial Security Manual.*

14. Security Classification Specifications for this solicitation / contract are identified below *("X" applicable box(es) and supply attachments as required)*. Any narrative or classification guide(s) furnished shall be annotated or have information appended to clearly and precisely identify each element of information which requires a classification. When a classification guide is utilized, that portion of the guide(s) pertaining to the specific contractual effort may be extracted and furnished the contractor. When a total guide(s) is utilized, each individual portion of the guide(s) which pertains to the contractual effort shall be clearly identified in Item 14b. The following information must be provided for each item of classified information identified in an extract or guide:

(I) Category of classification. (II) Date or event for declassification or review for declassification, and (III) The date or event for downgrading *(If applicable)*.

The official named in Item 12b, is responsible for furnishing the contractor copies of all guides and changes thereto that are made a part of this specification. Classified information may be attached or furnished under separate cover.

☐ a. A completed narrative is (1) ☐ attached, or (2) ☐ transmitted under separate cover and made a part of this specification.

☐ b. The following classification guide(s) is made a part of this specification and is (1) ☐ attached, or (2) ☐ transmitted under separate cover. *(List guides under Item 15 or in an attachment by title, reference number and date)*.

☐ c. Service-type contract/ subcontract. *(Specify instructions in accordance with ISR / ISM, as appropriate.)*.

☐ d. "X" only if this is a final specification and Item 6 is a "NO" answer. In response to the contractor's request dated ____________, retention of the identified classified material is authorized for a period of ____________.

☐ e. Annual review of this DD Form 254 is required. If "X'd" provide date such review is due: ____________.

15. Remarks *(Whenever possible, illustrate proper classification, declassification, and if applicable, downgrading instructions)*.

16a. Contract Security Classification Specifications for Subcontracts issuing from this contract will be approved by the Office named in Item 16e below, or by the prime contractor, as authorized. This Contract Security Classification Specification and attachments referenced herein are approved by the *User Agency* Contracting Officer or his Representative named in Item 16b below.

REQUIRED DISTRIBUTION:

- ☐ Prime Contractor *(Item 7a)*
  - ☐ Cognizant Security Office *(Item 7c)*
- ☐ Administrative Contracting Office *(Item 16e)*
  - ☐ Quality Assurance Representative
- ☐ Subcontractor *(Item 8a)*
  - ☐ Cognizant Security Office *(Item 8c)*
- ☐ Program/ Project Manager *(Item 12b)*
  - ☐ U.S. Activity Responsible for Overseas Security Administration

ADDITIONAL DISTRIBUTION:

☐

☐

☐

b. Typed name and title of approving official

c. Signature

d. Approving official's activity address and Zip Code

e. Name, address and Zip Code of Administrative Contracting Office

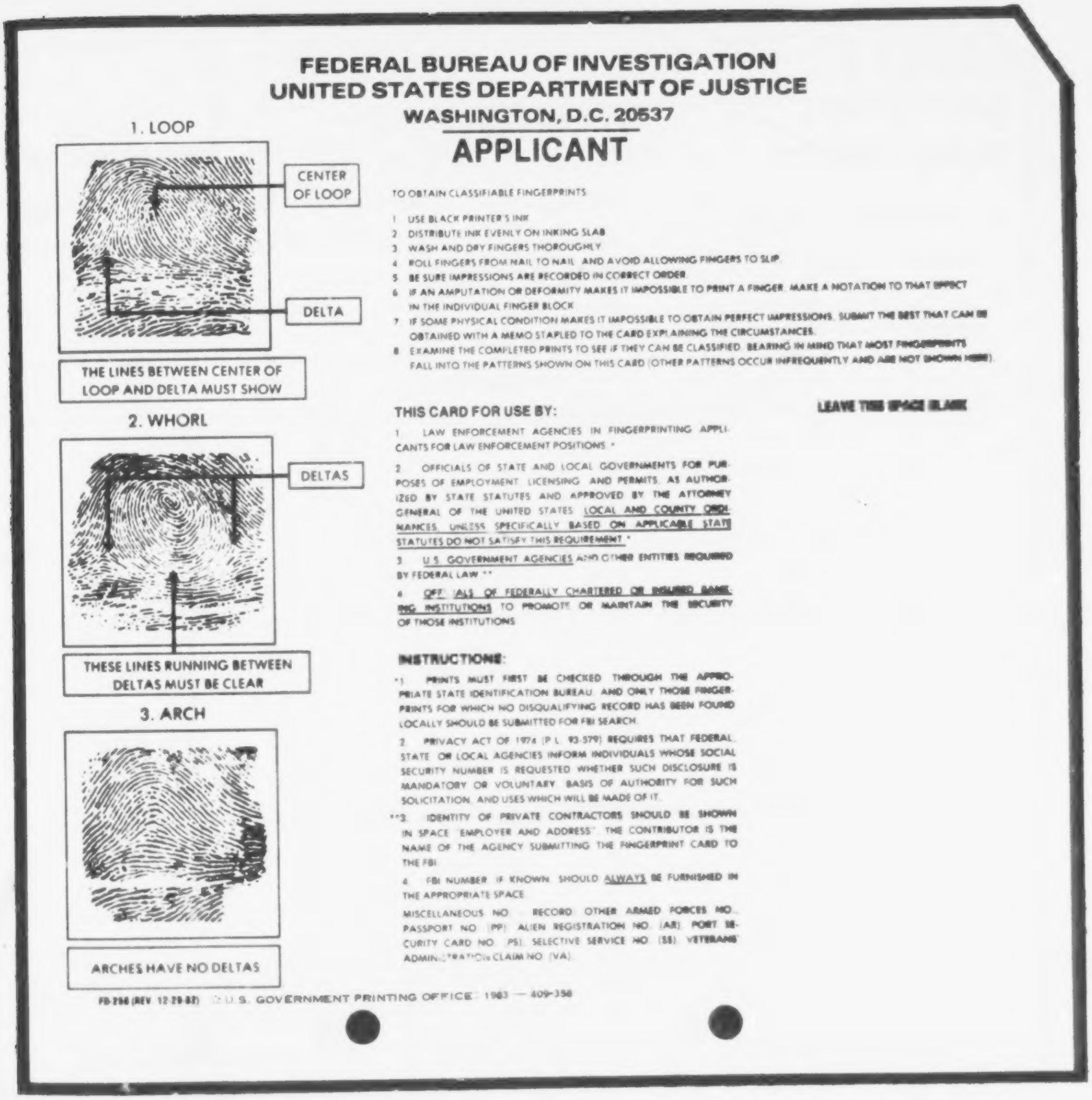
• U.S.GPO:[illegible]-0-163-[illegible]

DD Form 254 Reverse, JAN 78

H. "Applicant Fingerprint Card" (FD Form 258). This form is completed for all personnel being considered by DISCO for a PCL or an LAA. Completion of the form is a prerequisite to the granting of such actions. Care shall be exercised to ensure that fingerprints are authentic, legible, and complete, as forms that do not meet prescribed standards shall be returned for reexecution, which will result in clearance delays. For additional information, refer to paragraphs 26a(3) and 26b(3).)

SAMPLE

FD Form 258



FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20537

APPLICANT

1. LOOP

CENTER OF LOOP

DELTA

THE LINES BETWEEN CENTER OF LOOP AND DELTA MUST SHOW

2. WHORL

DELTAS

THESE LINES RUNNING BETWEEN DELTAS MUST BE CLEAR

3. ARCH

ARCHES HAVE NO DELTAS

TO OBTAIN CLASSIFIABLE FINGERPRINTS

1 USE BLACK PRINTER'S INK
2 DISTRIBUTE INK EVENLY ON INKING SLAB
3 WASH AND DRY FINGERS THOROUGHLY
4 ROLL FINGERS FROM NAIL TO NAIL AND AVOID ALLOWING FINGERS TO SLIP
5 BE SURE IMPRESSIONS ARE RECORDED IN CORRECT ORDER
6 IF AN AMPUTATION OR DEFORMITY MAKES IT IMPOSSIBLE TO PRINT A FINGER, MAKE A NOTATION TO THAT EFFECT IN THE INDIVIDUAL FINGER BLOCK
7 IF SOME PHYSICAL CONDITION MAKES IT IMPOSSIBLE TO OBTAIN PERFECT IMPRESSIONS, SUBMIT THE BEST THAT CAN BE OBTAINED WITH A MEMO STAPLED TO THE CARD EXPLAINING THE CIRCUMSTANCES.
8 EXAMINE THE COMPLETED PRINTS TO SEE IF THEY CAN BE CLASSIFIED, BEARING IN MIND THAT MOST FINGERPRINTS FALL INTO THE PATTERNS SHOWN ON THIS CARD (OTHER PATTERNS OCCUR INFREQUENTLY AND ARE NOT SHOWN HERE).

THIS CARD FOR USE BY:

1 LAW ENFORCEMENT AGENCIES IN FINGERPRINTING APPLICANTS FOR LAW ENFORCEMENT POSITIONS.*

2 OFFICIALS OF STATE AND LOCAL GOVERNMENTS FOR PURPOSES OF EMPLOYMENT, LICENSING, AND PERMITS, AS AUTHORIZED BY STATE STATUTES AND APPROVED BY THE ATTORNEY GENERAL OF THE UNITED STATES. LOCAL AND COUNTY ORDINANCES, UNLESS SPECIFICALLY BASED ON APPLICABLE STATE STATUTES DO NOT SATISFY THIS REQUIREMENT.*

3 U.S. GOVERNMENT AGENCIES AND OTHER ENTITIES REQUIRED BY FEDERAL LAW.**

4 OFFICIALS OF FEDERALLY CHARTERED OR INSURED BANKING INSTITUTIONS TO PROMOTE OR MAINTAIN THE SECURITY OF THOSE INSTITUTIONS.

LEAVE THIS SPACE BLANK

INSTRUCTIONS:

*1 PRINTS MUST FIRST BE CHECKED THROUGH THE APPROPRIATE STATE IDENTIFICATION BUREAU, AND ONLY THOSE FINGERPRINTS FOR WHICH NO DISQUALIFYING RECORD HAS BEEN FOUND LOCALLY SHOULD BE SUBMITTED FOR FBI SEARCH.

2 PRIVACY ACT OF 1974 (P.L. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY NUMBER IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.

**3. IDENTITY OF PRIVATE CONTRACTORS SHOULD BE SHOWN IN SPACE "EMPLOYER AND ADDRESS". THE CONTRIBUTOR IS THE NAME OF THE AGENCY SUBMITTING THE FINGERPRINT CARD TO THE FBI.

4 FBI NUMBER, IF KNOWN, SHOULD ALWAYS BE FURNISHED IN THE APPROPRIATE SPACE.

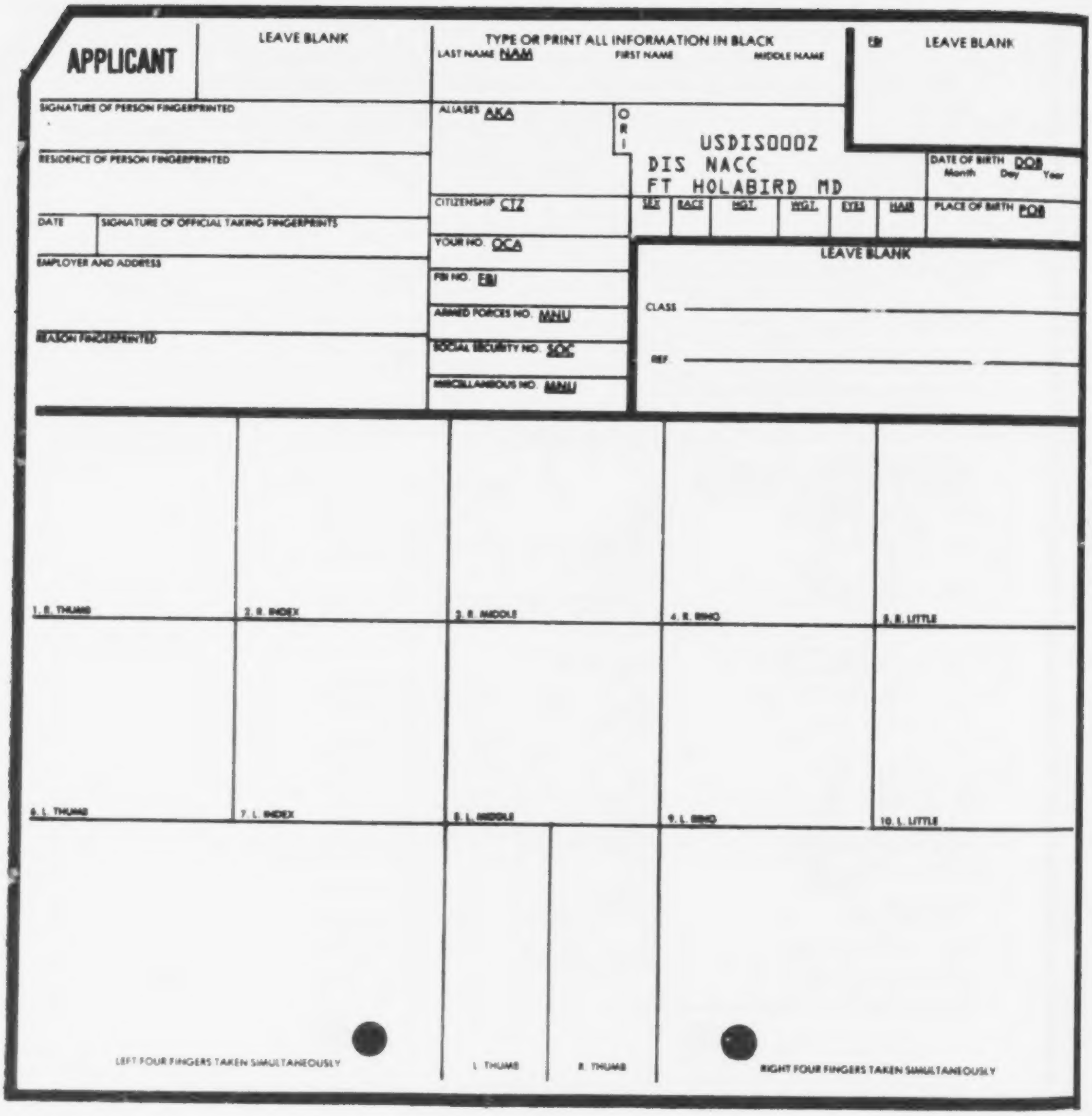
MISCELLANEOUS NO. - RECORD: OTHER ARMED FORCES NO., PASSPORT NO. (PP), ALIEN REGISTRATION NO. (AR), PORT SECURITY CARD NO. (PS), SELECTIVE SERVICE NO. (SS), VETERANS' ADMINISTRATION CLAIM NO. (VA).

FD-258 (REV. 12-29-82) ☆U.S. GOVERNMENT PRINTING OFFICE: 1983 — 409-358

SAMPLE

FD Form 258

Page Two



APPLICANT

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM FIRST NAME MIDDLE NAME

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED

ALIASES AKA

ORI USDIS0002Z
DIS NACC
FT HOLABIRD MD

RESIDENCE OF PERSON FINGERPRINTED

DATE OF BIRTH DOB Month Day Year

CITIZENSHIP CTZ

SEX RACE HGT. WGT. EYES HAIR

PLACE OF BIRTH POB

DATE

SIGNATURE OF OFFICIAL TAKING FINGERPRINTS

YOUR NO. OCA

LEAVE BLANK

EMPLOYER AND ADDRESS

FBI NO. FBI

CLASS

ARMED FORCES NO. MNU

REASON FINGERPRINTED

SOCIAL SECURITY NO. SOC

REF.

MISCELLANEOUS NO. MNU

1. R. THUMB
2. R. INDEX
3. R. MIDDLE
4. R. RING
5. R. LITTLE
6. L. THUMB
7. L. INDEX
8. L. MIDDLE
9. L. RING
10. L. LITTLE

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY

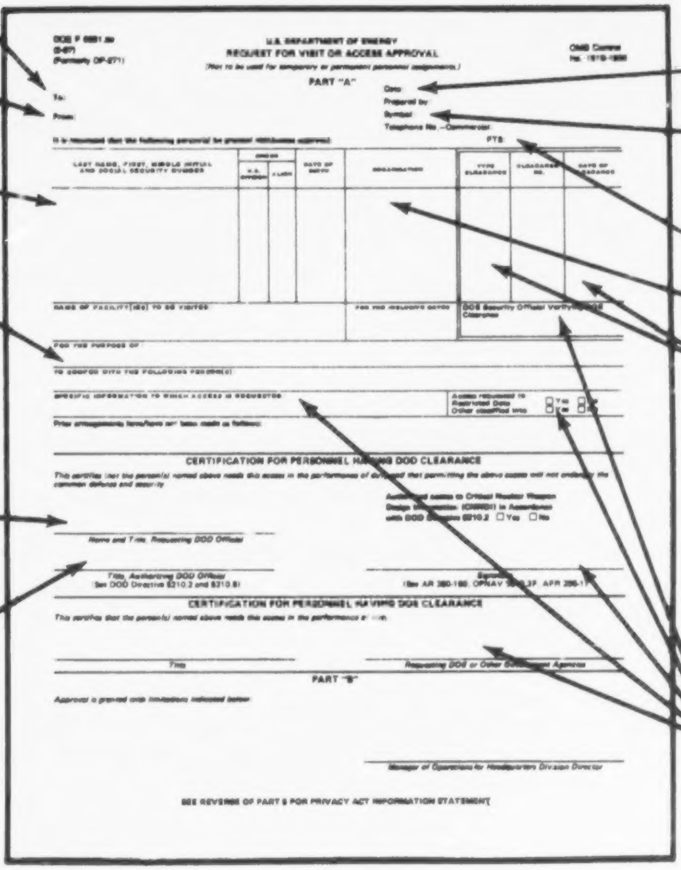
L. THUMB

R. THUMB

RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

I. "Request for Visit or Access Approval" (DOE F 5631.20). This form is included for information purposes. It is used for processing visits involving access to RESTRICTED DATA. Copies of this form may be obtained from the DOE.

SAMPLE



U.S. DEPARTMENT OF ENERGY
REQUEST FOR VISIT OR ACCESS APPROVAL

PART "A"

To:
From:
Date:
Prepared by:
Symbol:
FTS:

CERTIFICATION FOR PERSONNEL HAVING DOD CLEARANCE

CERTIFICATION FOR PERSONNEL HAVING DOE CLEARANCE

PART "B"

Insert the office and address of DOE Manager having operational control over the installation to be visited.

Insert contracting activity and address of User Agency supporting the visit request.

Enter the full name of each proposed visitor and his social security number.

State the purpose of the visit in sufficient detail to enable the addressee to ascertain the subject area involved, and to determine the level and scope of access required. Classified information will not be disclosed in this item.

To be signed, on the original only, by the contracting officer. Then forward to appropriate DOE Manager of operations.

Insert the signature block of the certifying official. Also show the position title of the certifying official (for example: A. B. Jones, Contracting Officer, Project Spoonfish, Naval Ship Systems Command, Main Navy Bldg., Washington, DC 20360).

Insert the date on which the form is prepared.

Enter symbol and telephone number of contracting officer of activity identified in "From" line.

Federal telephone system.

Name and address of contractor facility.

For each proposed visitor, show the current highest level of access he or she is authorized, and the date of its issuance. For contractor personnel, use the date of the current Letter of Consent (DISCO Form 560), which can be obtained from the contractor.

To be certified by the Facility Security Supervisor.

Leave blank; this space is for use by the activity to be visited.

PRIVACY ACT INFORMATION STATEMENT

Collection of the information requested is authorized by Section 145 of the Atomic Energy Act of 1954, as amended (PL 83-703, 42 USC 2165). Compliance with this request is voluntary; however, if the information submitted is inadequate or incomplete, approval for your visit to a classified DOE facility, or your access to classified information may be delayed or withheld. The information you furnish will be used by DOE and DOE contractors to control access to classified information and areas.

The social security number is not required for these purposes, but you may voluntarily furnish it to assist us in correct identification.

SAMPLE

J. "Letter of Notification of Facility Security Clearance" (DIS FL 381-R). This letter is used by the DIS to notify a facility that it has been granted an FCL. Letters of notification shall not be duplicated, and the fact that an FCL has been granted shall not be used for promotional or advertising purposes.

(Sample "Letter of Notification of Facility Security Clearance")
(Edition of January 1981 is obsolete.)

(Use appropriate DIS letterhead stationery.)

Name and Address of Facility

Dear ______________:

In reference to our earlier correspondence regarding the eligibility of your facility for a Department of Defense security clearance, I am pleased to advise that the necessary processing has been completed and security clearance at the ______________________ level is hereby granted to your facility.

The fact that your organization has qualified for and been granted a facility security clearance may not be used for advertising or promotional purposes, nor may this letter be reproduced in any form except for the necessary records of your organization.

As your cognizant security office, we are vitally interested in assisting you in the development of a sound security posture. We will conduct periodic reviews of your program to aid you in maintaining proper security safeguards. You may contact us for guidance or assistance.

Sincerely,

(Signature and Title)

DIS FL 381-R
Oct 83

K. Reserved.

L. "Department of Defense Security Agreement" (DD Form 441) and "Appendage" (DD Form 441-1). This form is used to obtain the formal agreement of management of a facility to abide by the DoD "Industrial Security Manual for Safeguarding Classified Information" (Attachment to DD Form 441). Once executed, a DD Form 441 continues in effect until terminated by one of the parties thereto, as provided for in section IV, "Termination," of the form. Execution of the DD Form 441 is a prerequisite to the processing of an FCL. An appendage (DD Form 441-1), to be used when management desires to indicate multiple facility coverage with one "DD Form 441," is included herewith. After a "Department of Defense Security Agreement" has been properly executed, a contractor may use the DD Form 441-1 to accomplish additions, deletions, or changes in the branches and/or facilities included in and covered by the DD Form 441. After the HOF of the MFO has executed the DD Form 441, it is permissible for one of the executive personnel at the specific operating location of the company, including the FSO, to sign the DD Form 441-1. This authority may be exercised by the local management official, provided he or she has the delegated authorization to do so, whether or not the official is also an officer of the company.

SAMPLE

DD Form 441

DEPARTMENT OF DEFENSE

SECURITY AGREEMENT

Form Approved
OMB No. 0704-0194
Expires Apr 30, 1990

THIS DEPARTMENT OF DEFENSE SECURITY AGREEMENT *(hereinafter called the Agreement)*, entered into this ____________ day of ________________ 19 _____, by and between THE UNITED STATES OF AMERICA through the Defense Investigative Service acting for the Department of Defense and other governmental User Agencies *(hereinafter called the Government)*, and

(1) a corporation organized and existing under the laws of the state of ________________________________

(2) a partnership consisting of ________________________________

(3) an individual trading as ________________________________

with its principal office and place of business at *(Street, city, state and ZIP code)*

____

(hereinafter called the Contractor)

WITNESSETH THAT:

WHEREAS, the Government has in the past purchased or may in the future purchase from the Contractor supplies or services, which are required and necessary to the national security of the United States, or may invite bids or request quotations on proposed contracts for the purchase of supplies or services, which are required and necessary to the national security of the United States, and

WHEREAS, it is essential that certain security measures be taken by the Contractor prior to and after being accorded access to classified information, and

WHEREAS, the parties desire to define and set forth the precautions and specific safeguards to be taken by the Contractor and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information, sabotage, or any other acts detrimental to the security of the United States,

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree as follows

Section I - SECURITY CONTROLS

(A) The Contractor agrees to provide and maintain a system of security controls within the organization in accordance with the requirements of the Department of Defense "Industrial Security Manual for Safeguarding Classified Information" (hereinafter called the Manual) attached hereto and made a part of this agreement, subject, however, (i) to any revisions of the Manual required by the demands of national security as determined by the Government, notice of which shall be furnished to the Contractor, and (ii) to mutual agreements entered into by the parties in order to adapt the Manual to the Contractor's business and necessary procedures thereunder. In order to place in effect such security controls, the Contractor further agrees to prepare Standard Practice Procedures for internal use, such procedures to be consistent with the Manual. In the event of any inconsistency between the Manual, as revised, and the Contractor's Standard Practice Procedures, the Manual shall control.

(B) The Government agrees that it shall indicate when necessary, by security classification (TOP SECRET, SECRET, or CONFIDENTIAL), the degree of importance to the national security of information pertaining to supplies, services, and other matters to be furnished by the Contractor to the Government or by the Government to the Contractor, and the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof; provided, however, that matters requiring security classification will be assigned the least restricted security classification consistent with proper safeguarding of the matter concerned, since over-classification causes unnecessary operational delays and depreciates the importance of correctly classified matter. Further, the Government agrees that when Atomic Energy information is involved it will, when necessary, indicate by a marking additional to the classification marking that the information is "RESTRICTED DATA." The "Department of Defense Contract Security Classification Specification" (DD Form 254) is the basic document by which classification, regrading, and declassification specifications are documented and conveyed to the Contractor.

(C) The Government agrees, on written application, to grant personnel security clearances to eligible employees of the Contractor who require access to information classified TOP SECRET, SECRET, or CONFIDENTIAL.

(D) The Contractor agrees to determine that any subcontractor, subbidder, individual, or organization proposed for the furnishing of supplies or services which will involve access to classified information, has been granted an appropriate Department of Defense facility security clearance, which is still in effect prior to according access to such classified information.

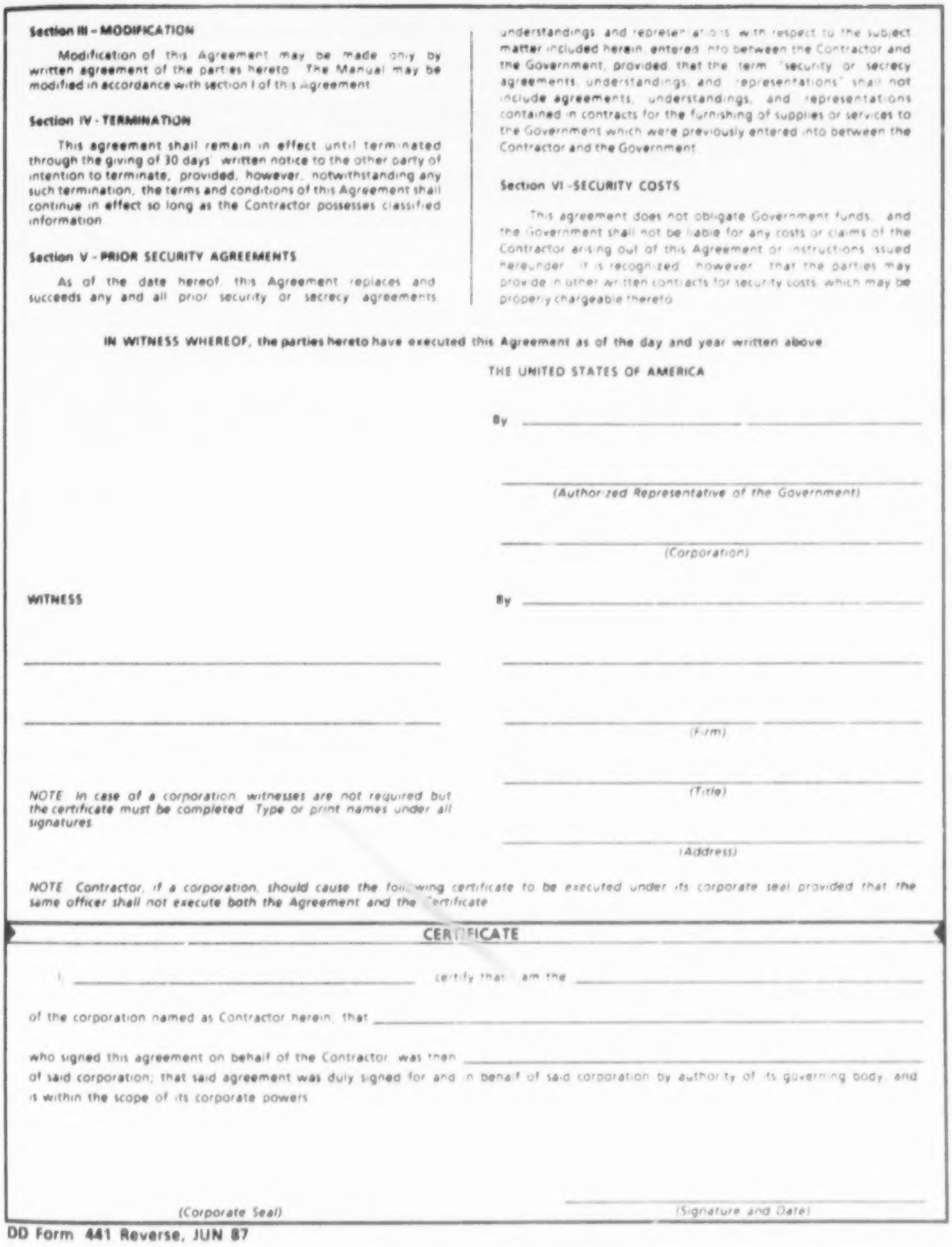
Section II - INSPECTION

Designated representatives of the Government responsible for inspection pertaining to industrial plant security shall have the right to inspect, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Manual. Should the Government, through its authorized representative, determine that the Contractor's security methods, procedures, or facilities do not comply with such requirements, it shall submit a written report to the Contractor advising of the deficiencies.

DD Form **441, JUN 87** *Previous editions are obsolete*

SAMPLE

DD Form 441
Page Two



Section III - MODIFICATION

Modification of this Agreement may be made only by written agreement of the parties hereto. The Manual may be modified in accordance with section I of this Agreement.

Section IV - TERMINATION

This agreement shall remain in effect until terminated through the giving of 30 days' written notice to the other party of intention to terminate, provided, however, notwithstanding any such termination, the terms and conditions of this Agreement shall continue in effect so long as the Contractor possesses classified information.

Section V - PRIOR SECURITY AGREEMENTS

As of the date hereof, this Agreement replaces and succeeds any and all prior security or secrecy agreements understandings and representations with respect to the subject matter included herein, entered into between the Contractor and the Government, provided that the term "security or secrecy agreements, understandings and representations" shall not include agreements, understandings, and representations contained in contracts for the furnishing of supplies or services to the Government which were previously entered into between the Contractor and the Government.

Section VI - SECURITY COSTS

This agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs, which may be properly chargeable thereto.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year written above.

THE UNITED STATES OF AMERICA

By ______________________ ______________________

____
(Authorized Representative of the Government)

____
(Corporation)

WITNESS

____

____

By ______________________

____

______________________ ______________________
(Firm)

____
(Title)

____
(Address)

NOTE: In case of a corporation, witnesses are not required but the certificate must be completed. Type or print names under all signatures.

NOTE: Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, ______________________ certify that I am the ______________________

of the corporation named as Contractor herein; that ______________________

who signed this agreement on behalf of the Contractor, was then ______________________ of said corporation; that said agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

____
(Signature and Date)

DD Form 441 Reverse, JUN 87

SAMPLE

DD Form 441-1

APPENDAGE TO DEPARTMENT OF DEFENSE SECURITY AGREEMENT	*Form Approved* *OMB No. 0704-0194* *Expires Apr 30, 1990*

It is further agreed, on this__________day of_____________19____, by and between the United States of America through the Defense Investigative Service, acting for the Department of Defense, hereafter called the Government, and ____which has entered into the Security Agreement to which this appendix is made a part that the branches and/or facilities listed below, owned and/or operated by said contractor are included in and covered by the provisions of the said Security Agreement, and Certificate Pertaining to Foreign Affiliation, DD Form 441s

NAME OF PLANT OR FACILITY	NUMBER AND STREET ADDRESS	CITY AND STATE

THE UNITED STATES OF AMERICA	CONTRACTOR
BY	BY *(Authorized Representative of Contractor)*
AUTHORIZED REPRESENTATIVE OF THE GOVERNMENT	TITLE
	ADDRESS

DD Form 441-1, JUN 87 *Previous editions are obsolete*

M. "Certificate Pertaining to Foreign Interests" (DD Form 441s). This form is used to provide formal certification from the contractor relative to FOCI, in order that the DoD may determine eligibility for an FCL. In completing the DD Form 441s, all items are to be answered by indicating "X" in either the "Yes" or "No" column. If an answer to any question is "Yes," the following paragraphs provide instructions for the submission of necessary data.

Question 1. Identify the percentage of any class of shares or other securities issued, that is owned by foreign interests, broken down by country. If the answer is "Yes" and a copy of Schedule 13D and/or Schedule 13G filed by the investor with the Securities and Exchange Commission (SEC), has been received, attach a copy of Schedule 13D and/or Schedule 13G to the revised DD Form 441s.

Question 2. Furnish the name, address by country, and the percentage owned. Include name and title of officials of the facility who occupy positions with the foreign entity, if any. If none, so state.

Question 3. Furnish full information concerning the identity of the foreign interest, and the position he or she holds in the organization.

Question 4. Identify the foreign interest(s) and furnish full details concerning the control or influence.

Question 5. Furnish name of foreign interest, country, and nature of agreement or involvement. Agreements include licensing, sales, patent exchange, trade secrets, agency, cartel, partnership, joint venture, and proxy.

Question 6. Furnish the amount of indebtedness and by whom furnished as related to the current assets of the organization. Include specifics as to the type of indebtedness and what, if any, collateral, including voting stock, has been furnished or pledged. If any debentures are convertible, specifics are to be furnished.

Question 7. State full particulars with respect to any income from Designated countries, including percentage from each such country, as related to total income, and the type of services or products involved. If income is from non-Designated countries, give overall percentage as related to total income and type of services or products in general terms. If income is from a number of foreign countries, identify countries and include percentage of income by each country.

Question 8. Identify each foreign institutional investor holding 5 percent or more of the voting stock. Identification should include the name and address of the investor and percentage of stock held. State whether the investor has attempted to, or has in fact, exerted any management control or influence over the appointment of directors, officers, or other key management personnel, and whether such investors have attempted to influence the policies of the corporation. If a copy of Schedule 13D and/or Schedule 13G filed by the investor with the SEC has been received, attach a copy of Schedule 13D and/or Schedule 13G to the revised DD Form 441s.

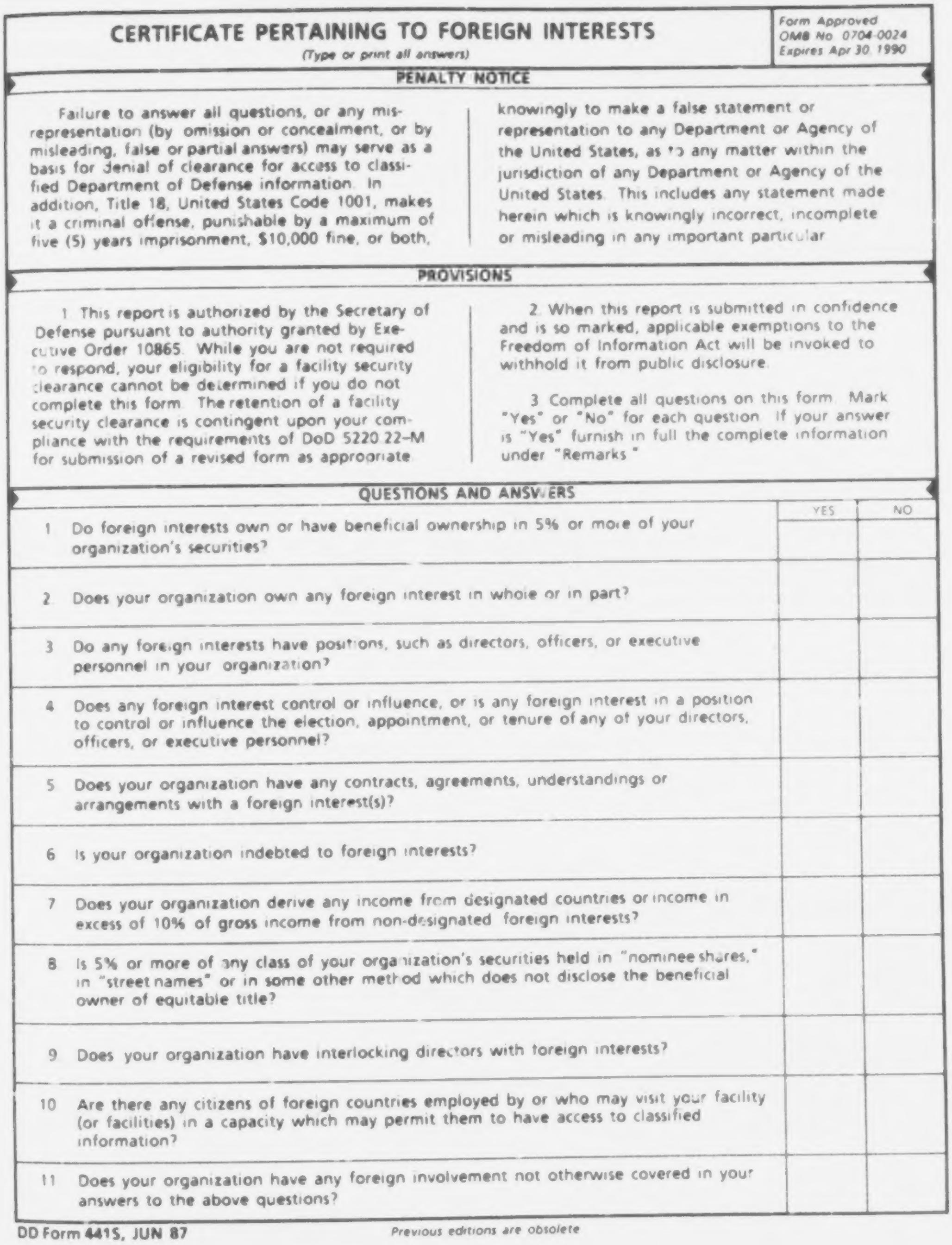
Question 9. Include identifying data on all such directors. If they have a security clearance, state so. Also, indicate the name and address of all other corporations with which they serve in any capacity.

Question 10. Provide complete information by identifying the individuals and the country of which they are a citizen. Category 4 (see paragraph 41d) visits are not included in the range of this question.

Question 11. Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

SAMPLE

DD Form 441s



CERTIFICATE PERTAINING TO FOREIGN INTERESTS

(Type or print all answers)

Form Approved
OMB No. 0704-0024
Expires Apr 30 1990

PENALTY NOTICE

Failure to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, $10,000 fine, or both, knowingly to make a false statement or representation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.

PROVISIONS

1. This report is authorized by the Secretary of Defense pursuant to authority granted by Executive Order 10865. While you are not required to respond, your eligibility for a facility security clearance cannot be determined if you do not complete this form. The retention of a facility security clearance is contingent upon your compliance with the requirements of DoD 5220.22-M for submission of a revised form as appropriate.

2. When this report is submitted in confidence and is so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold it from public disclosure.

3. Complete all questions on this form. Mark "Yes" or "No" for each question. If your answer is "Yes" furnish in full the complete information under "Remarks."

QUESTIONS AND ANSWERS

	YES	NO
1 Do foreign interests own or have beneficial ownership in 5% or more of your organization's securities?		
2. Does your organization own any foreign interest in whole or in part?		
3 Do any foreign interests have positions, such as directors, officers, or executive personnel in your organization?		
4 Does any foreign interest control or influence, or is any foreign interest in a position to control or influence the election, appointment, or tenure of any of your directors, officers, or executive personnel?		
5 Does your organization have any contracts, agreements, understandings or arrangements with a foreign interest(s)?		
6 Is your organization indebted to foreign interests?		
7 Does your organization derive any income from designated countries or income in excess of 10% of gross income from non-designated foreign interests?		
8 Is 5% or more of any class of your organization's securities held in "nominee shares," in "street names" or in some other method which does not disclose the beneficial owner of equitable title?		
9 Does your organization have interlocking directors with foreign interests?		
10 Are there any citizens of foreign countries employed by or who may visit your facility (or facilities) in a capacity which may permit them to have access to classified information?		
11 Does your organization have any foreign involvement not otherwise covered in your answers to the above questions?		

DD Form 441S, JUN 87 *Previous editions are obsolete*

SAMPLE
DD Form 441s
Page Two

REMARKS *(Attach additional sheets, if necessary, for a full detailed statement.)*

CERTIFICATION

I CERTIFY that the entries made by me above are true, complete, and correct to the best of my knowledge and belief and are made in good faith.

WITNESS:

______________________ ______________________
(Date Certified)

______________________ By ______________________

____
(Contractor)

____
(Title)

NOTE *In case of corporation, witnesses not required but certificate below must be completed. Type or print names under all signatures.*

____
(Address)

NOTE *Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the agreement and the certificate.*

CERTIFICATE

I, ______________________ certify that I am the ______________________ of the corporation named as Contractor herein; that ______________________ who signed this certificate on behalf of the Contractor, was then ______________________ of said corporation; that said certificate was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

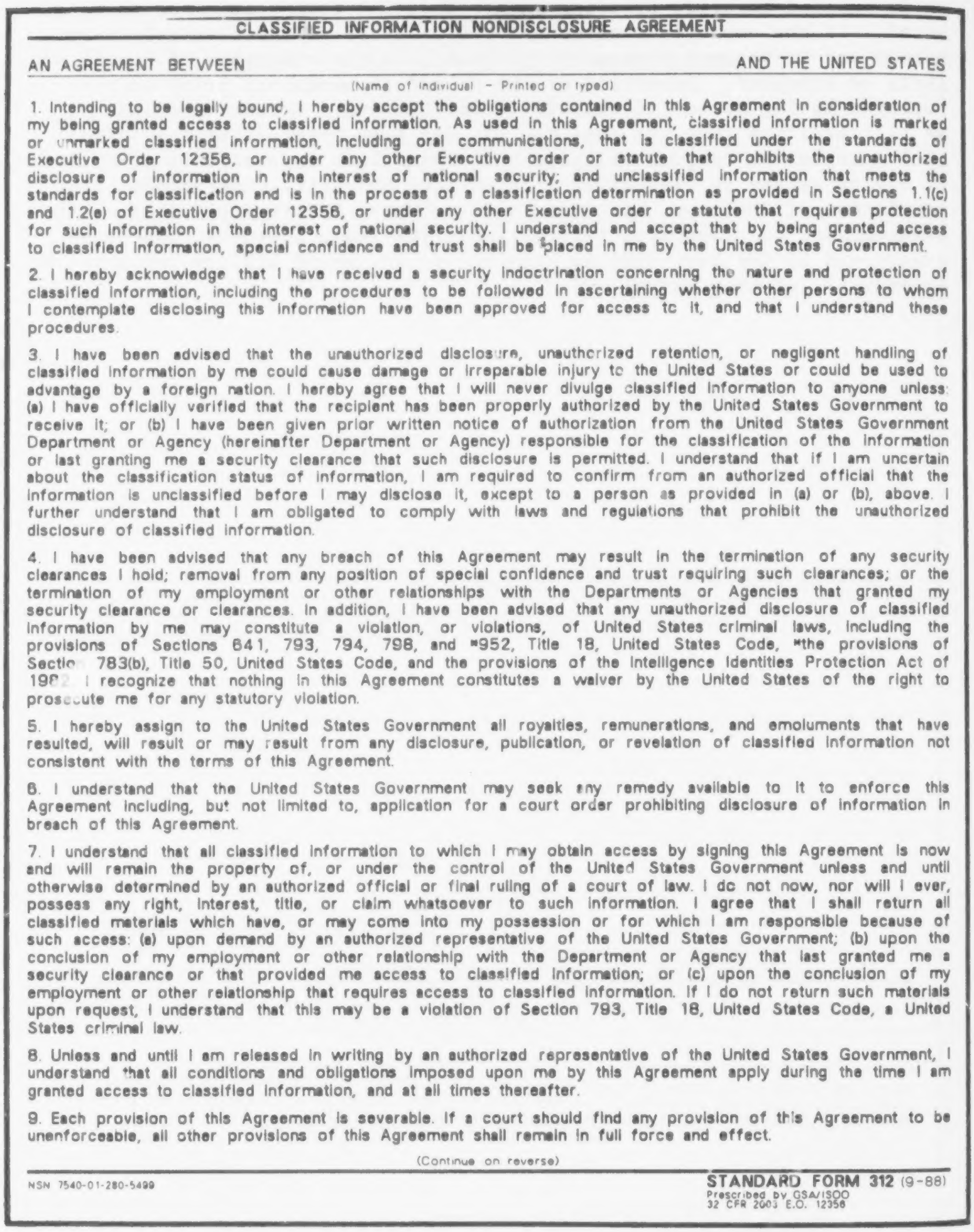
____
(Signature and Date)

DD Form 441S Reverse, JUN 87

N. "Classified Information Nondisclosure Agreement," Standard Form (SF) 312. This form shall be executed by all contractor employees following their initial security briefing and at the time their clearance is terminated. If the employee's personnel clearance is administratively terminated, and it becomes necessary to revalidate the clearance, a new SF 312 shall be executed. Execution of the SF 312 is mandatory prior to the employee having access to classified information. Execution of the SF 312 certifies that the employee (i) has been briefed (or debriefed); (ii) accepts the responsibilities and limitations imposed as a condition of having access to classified information; and (iii) understands the provisions of the laws, statutes, and executive orders applicable to the safeguarding of classified information. The laws, statutes, executive orders and 32 CFR Part 2003 as referred to in the SF 312 are contained in appendix VI of this manual.

SAMPLE

Standard Form 312



CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN ______ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse)

NSN 7540-01-280-5499

STANDARD FORM 312 (9-88)
Prescribed by GSA/ISOO
32 CFR 2003 E.O. 12356

SAMPLE

Standard Form 312

Page Two

10. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *Section 783(b), Title 50, United States Code, the Intelligence Identities Protection Act of 1982, Executive Order 12356 or its successor, and Section 2003.20, Title 32, Code of Federal Regulations, so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.
SIGNATURE DATE	SIGNATURE DATE
NAME AND ADDRESS (Type or print)	NAME AND ADDRESS (Type or print)

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

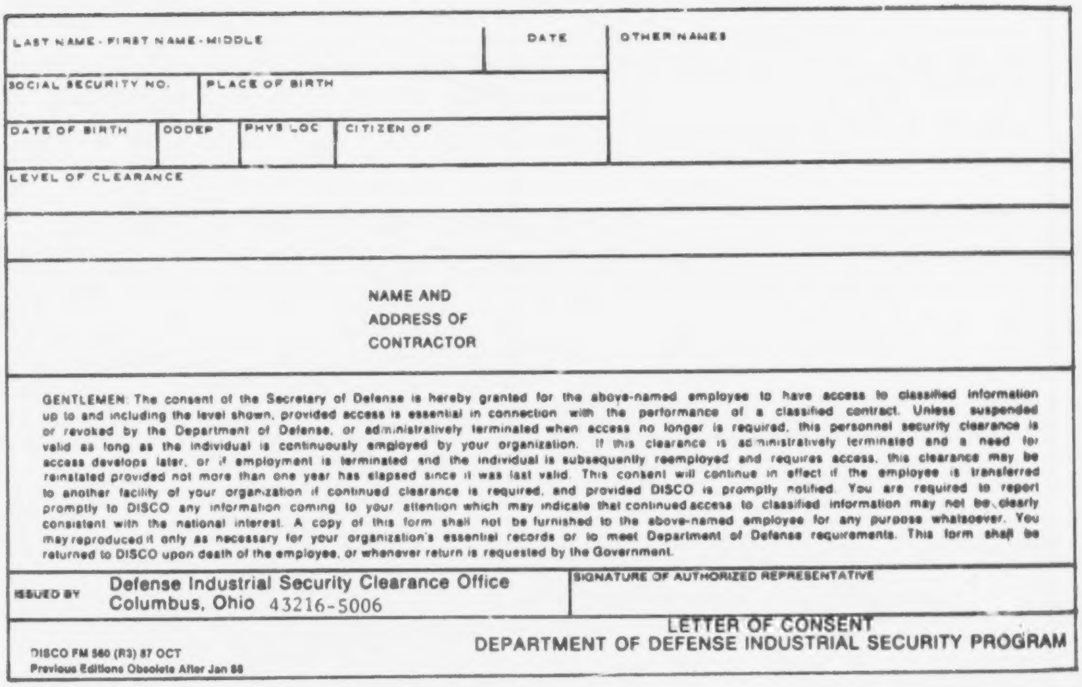
NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (9-88)

O. "Letter of Consent" (DISCO Form 560). The LOC is used by DISCO to notify a facility that one of its employees is authorized to have access to classified information of the category indicated. LOC's are not issued to individuals; therefore, this form shall not be released to employees. The DISCO Form 560 may be transmitted to the employing contractor by the U.S. Postal Service, or electronically via CompuServe.

SAMPLE



LAST NAME - FIRST NAME - MIDDLE
DATE
OTHER NAMES
SOCIAL SECURITY NO.
PLACE OF BIRTH
DATE OF BIRTH
OODEP
PHYS LOC
CITIZEN OF
LEVEL OF CLEARANCE

NAME AND
ADDRESS OF
CONTRACTOR

GENTLEMEN: The consent of the Secretary of Defense is hereby granted for the above-named employee to have access to classified information up to and including the level shown, provided access is essential in connection with the performance of a classified contract. Unless suspended or revoked by the Department of Defense, or administratively terminated when access no longer is required, this personnel security clearance is valid as long as the individual is continuously employed by your organization. If this clearance is administratively terminated and a need for access develops later, or if employment is terminated and the individual is subsequently reemployed and requires access, this clearance may be reinstated provided not more than one year has elapsed since it was last valid. This consent will continue in effect if the employee is transferred to another facility of your organization if continued clearance is required, and provided DISCO is promptly notified. You are required to report promptly to DISCO any information coming to your attention which may indicate that continued access to classified information may not be clearly consistent with the national interest. A copy of this form shall not be furnished to the above-named employee for any purpose whatsoever. You may reproduce it only as necessary for your organization's essential records or to meet Department of Defense requirements. This form shall be returned to DISCO upon death of the employee, or whenever return is requested by the Government.

ISSUED BY Defense Industrial Security Clearance Office
Columbus, Ohio 43216-5006

SIGNATURE OF AUTHORIZED REPRESENTATIVE

LETTER OF CONSENT
DEPARTMENT OF DEFENSE INDUSTRIAL SECURITY PROGRAM

DISCO FM 560 (R3) 87 OCT
Previous Editions Obsolete After Jan 88

P. Reserved.

Q. "Personnel Security Clearance Change Notification" (DISCO Form 562). This is a multipurpose form used by the contractor to report one of the following occurrences concerning a cleared employee or an employee for whom a clearance has been requested. The form shall be submitted to DISCO, except when the individual concerned is either cleared or in the process of being cleared in connection with the FCL in which case the form shall be submitted to the CSO. The CSO, after annotating its own records, will forward the form to DISCO. Only one legible copy of the form is required to be submitted. In the case of a multiple facility transfer, DISCO will acknowledge its receipt using an appropriate form letter. In the case of a change of name, DISCO will issue a new LOC.

1. Clearance transfers within an MFO (see paragraph 26e) -- the name and address of the facility to which the individual is to be transferred shall be included in the "Remarks" block of the form. The name and address of the submitting facility, if different from block 4, shall also be listed and identified in the "Remarks" portion of the form. It should be noted that where a contractor in an MFO elects, pursuant to paragraph 26h(2), to have all LOC's issued to the HOF or a PMF, the name and address of the facility at which the individual is employed will be placed in the "Name, Address, CAGE Code and Telephone Number of Employer" block of the DISCO Form 562. In addition, the name and address of the facility to which LOC's are to be mailed shall be placed in the "Remarks" block of the form preceded by the words "MAIL TO" in bold letters. (see paragraph 26h(2)(c)).

2. Change of name (see paragraph 26h(1)(e) -- the name of the individual exactly as shown on the LOC (or on the DD Form 48, 48-3, or 49, in the case of an individual who is in the process of being cleared by DISCO) shall be placed in the "Name of Employee" block of the form. The individual's new name shall be set out in the "Remarks" block of the form. If the contractor has elected, under paragraph 26h(2), to have the LOC sent to a facility other than the one at which the individual is employed, the name and address of that facility shall be identified in the "Job Title" block.

3. Report of termination of employment (see paragraphs 6a(4)(c) and 6b(2)) -- indicate "Termination (date)" in the "Remarks" block of the form, if it is different from the effective date listed in block 2.

4. Downgrading or upgrading of a TOP SECRET or SECRET clearance *
(see paragraph 30) -- in the "Remarks" block indicate, "Downgrade without *
prejudice (or upgrade, as appropriate) to (TOP SECRET, SECRET or *
CONFIDENTIAL)."

5. Administrative termination of PCL's or LAA's that are no longer required -- (see paragraph 29).

SAMPLE

DISCO Form 562

PERSONNEL SECURITY CLEARANCE CHANGE NOTIFICATION

FORM APPROVED
OMB NO. 0704-0275
EXP. DATE: APR 30, 1990

1. TYPE OF ACTION *(" X" appropriate action box)*

☐ A. MULTIPLE FACILITY TRANSFER ☐ B. REINSTATEMENT ☐ C. REVALIDATION
☐ D. TERMINATION ☐ E. ADMINISTRATIVE TERMINATION ☐ F. DOWNGRADE
☐ G. CITIZENSHIP CHANGE *(See "Remarks")* ☐ H. SSN CORRECTION ☐ I. REQUEST FOR DUPLICATE LETTER OF CONSENT
☐ J. CHANGE OF NAME ☐ K. EMPLOYEE STATUS CHANGE ☐ L. DATE AND PLACE OF BIRTH CHANGE
☐ M. COLLOCATED FACILITY TRANSFER ☐ N. OTHER *(Indicate specific action, e.g., concurrent clearance, etc.)*

2. EFFECTIVE DATE OF ACTION "X'D" IN ITEM NO. 1

3. TERMINATION STATUS *(Complete if Item 1D or 1E is "X'd")*

☐ ACTIVE CLEARANCE ☐ PENDING CLEARANCE AND ☐ DD FORM 48 SUBMITTED ☐ DD FORM 48-3 SUBMITTED

4. NAME, ADDRESS AND ZIP CODE OF EMPLOYER	4A. CAGE CODE/FSC	5. NAME OF EMPLOYEE *(Last, First, Middle)*
	4B. TELEPHONE NO. *(Include Area Code)*	6. ANY OTHER NAME BY WHICH KNOWN *(Alias, Maiden, or Former Legal Name; Designate which)*

7. DATE OF BIRTH	8. PLACE OF BIRTH	9. CITIZEN OF *(Country)*	10. SOCIAL SECURITY NUMBER

11. CURRENT CLEARANCE INFORMATION INCLUDING COMPANY CONFIDENTIAL CLEARANCE

A. DEGREE OF CLEARANCE	B. DATE OF CLEARANCE	C. CLEARED BY

12. IS EMPLOYEE CLEARED OR IN PROCESS FOR CLEARANCE IN CONNECTION WITH FACILITY SECURITY CLEARANCE (OODEP) (SEE PAR. 22, ISM)

☐ YES ☐ NO *(If "Yes", enter Job Title in Item 13 and submit this form to Cognizant Security Office rather than DISCO.)*

13. JOB TITLE *(Complete this item only if item 12 is answered YES)*

14. **REMARKS** *(State appropriate information, i.e., Name and Address of Facility to which transferred; New Name of Employee - Last Name, First Name, Middle Name; list Concurrent clearance information; if death has occurred, state "Deceased" and include date of death; attach the Letter of Consent of the deceased to this form; indicate special situations, e.g., where employee is physically located if not the same as initiating facility shown in block 4, location to which employee is transferred, etc.) (If terminating pending government - granted clearance but retaining a company CONFIDENTIAL clearance, so indicate. If citizenship has changed, indicate certificate number, date, city and state of naturalization; name of court.*

15. "X" BOX "A" FOR ADMINISTRATIVE TERMINATION OR BOX "B" FOR ALL OTHER CHANGE NOTIFICATIONS

☐ A. I CERTIFY THAT THE ABOVE NAMED EMPLOYEE DOES NOT REQUIRE ACCESS TO CLASSIFIED INFORMATION IN CONNECTION WITH HIS (HER) EMPLOYMENT MOREOVER THERE WILL BE NO REQUIREMENT FOR THE EMPLOYEE TO HAVE ACCESS TO CLASSIFIED INFORMATION IN THE FORESEEABLE FUTURE ACCORDINGLY IT IS RECOMMENDED THAT THE PERSONNEL SECURITY CLEARANCE BE ADMINISTRATIVELY TERMINATED SINCE THERE IS NO CURRENT OR FORESEEABLE FUTURE PROCUREMENT REQUIREMENT FOR THE CLEARANCE IT IS UNDERSTOOD THIS RECOMMENDATION IS PURELY OF AN ADMINISTRATIVE NATURE AND DOES NOT REFLECT ADVERSELY ON THE EMPLOYEE IN ANY MANNER WHATSOEVER I CERTIFY THAT THE ENTRIES MADE ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF

☐ B. I CERTIFY THAT THE ENTRIES MADE ABOVE ARE TRUE, COMPLETE, AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF

C. SIGNATURE OF SECURITY SUPERVISOR	D. DATE

DISCO Form 562, Oct 86 Previous editions are obsolete.

R. Reserved.

S. Reserved.

T. 1. "Department of Defense Transportation Security Agreement" (DIS Form 1149). This form is prescribed for use by the CSO in obtaining the formal agreement of the HOF of the commercial carrier to abide by the ISM and the DoD 5220.22-C, "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information." Once executed, a DIS Form 1149 continues in effect until terminated by one of the parties thereto, as provided for in "Section VI - Termination," of the form. As long as the DIS Form 1149 is in effect, the carrier shall not be required to execute another form, unless there is a change in operating name or location of the HOF or reincorporation. Execution of the DIS Form 1149 is a prerequisite to making an eligibility determination with regard to transportation of SECRET controlled shipments.

2. "Appendage to Department of Defense Transportation Security Agreement" (DIS Form 1150). This form shall be used by management of the HOF of the commercial carrier to indicate those terminals covered by the DIS Form 1149. More information on both forms is available in DoD 5220.22-C, "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information." *

SAMPLE

DIS Form 1149

DEPARTMENT OF DEFENSE

TRANSPORTATION SECURITY AGREEMENT

FORM APPROVED
OMB NO. 0704-0199
EXP. DATE: APR 30, 1990

THIS AGREEMENT, entered into this __________ day of ____________________ 19 ____

by and between THE UNITED STATES OF AMERICA through the Defense Investigative Service acting for the Department of Defense Agencies and other user agencies, *(hereinafter called the Government)* and

(i) the following named corporation: ______________________________

____

organized and existing under the laws of the State of ______________________________

(ii) a partnership consisting of ______________________________

(iii) an individual trading as ______________________________

with its principal office and place of business at ______________________________

in the City of ____________________, State of ____________________ *(hereinafter called Carrier).*

WITNESSETH THAT:

WHEREAS, the Carrier is authorised by law, regulatory body or regulation to transport property; and

WHEREAS, the requirement for the Carrier's service has been established by a shipping component; and

WHEREAS, Military Traffic Management Command (MTMC) has determined that the Carrier meets current qualification requirements; and

WHEREAS, the Government has SECRET material to be transported *(hereinafter called SECRET Controlled Shipments)*; and

WHEREAS, it is essential that certain security measures be taken by the Carrier prior to, and after, his being accorded custody of SECRET Controlled Shipments; and

WHEREAS, the parties desire to define and set forth the precautions and specific safeguards to be taken by the Carrier and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of the contents of SECRET Controlled Shipments, sabotage, or any other such act detrimental to the security of the United States regarding such shipments.

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree, as follows:

SECTION I - SECURITY CONTROLS

(A) The carrier agrees to provide and maintain a system of security controls in accordance with the requirements of the Department of Defense Industrial Security Manual for safeguarding Classified Information and the Carrier Supplement thereto, *(hereinafter referred to as the Manual)* attached hereto and made and made a part of this Agreement, subject, however, to any revision of the Manual required by the demands of national security as determined by the Government, notice and copy of which will be furnished to the Carrier.

(B) The Carrier agrees to place in effect such security controls, by preparing Standard Practice Procedures such procedures to be consistent with the Manual. The Carrier's Standard Practice Procedures shall be subject to review by the Government. Such procedures are a prerequisite to the granting of a facility security clearance.

(C) The Carrier agrees to comply with all requirements and conditions set forth in the Manual applicable to the type of transportation being furnished for the movement of SECRET Controlled Shipments.

(D) The Carrier agrees that he shall not use the services of another business entity, which will envolve a SECRET Controlled Shipment entrusted to the Carrier named herein, without the the specific authorization of the Government.

(E) The Government agrees that it shall, via shipping order or bill of lading, indicate which shipments require the protection agreed to herein.

(F) The government agrees that if the Carrier meets the requirements of the Manual and this Agreement, it shall be granted authority to transport SECRET Controlled Shipments. Such authorization shall be made a matter of record in the files of MTMC and the Defense Supply Agency.

SECTION II - APPLICABILITY

(A) This Agreement applies only to the specific locations of the Carrier which have been authorized by the Government for handling SECRET Controlled Shipments and listed on the Appendage hereto.

(B) This Agreement does not apply to other Carriers or brokers acting as agents for the Carrier.

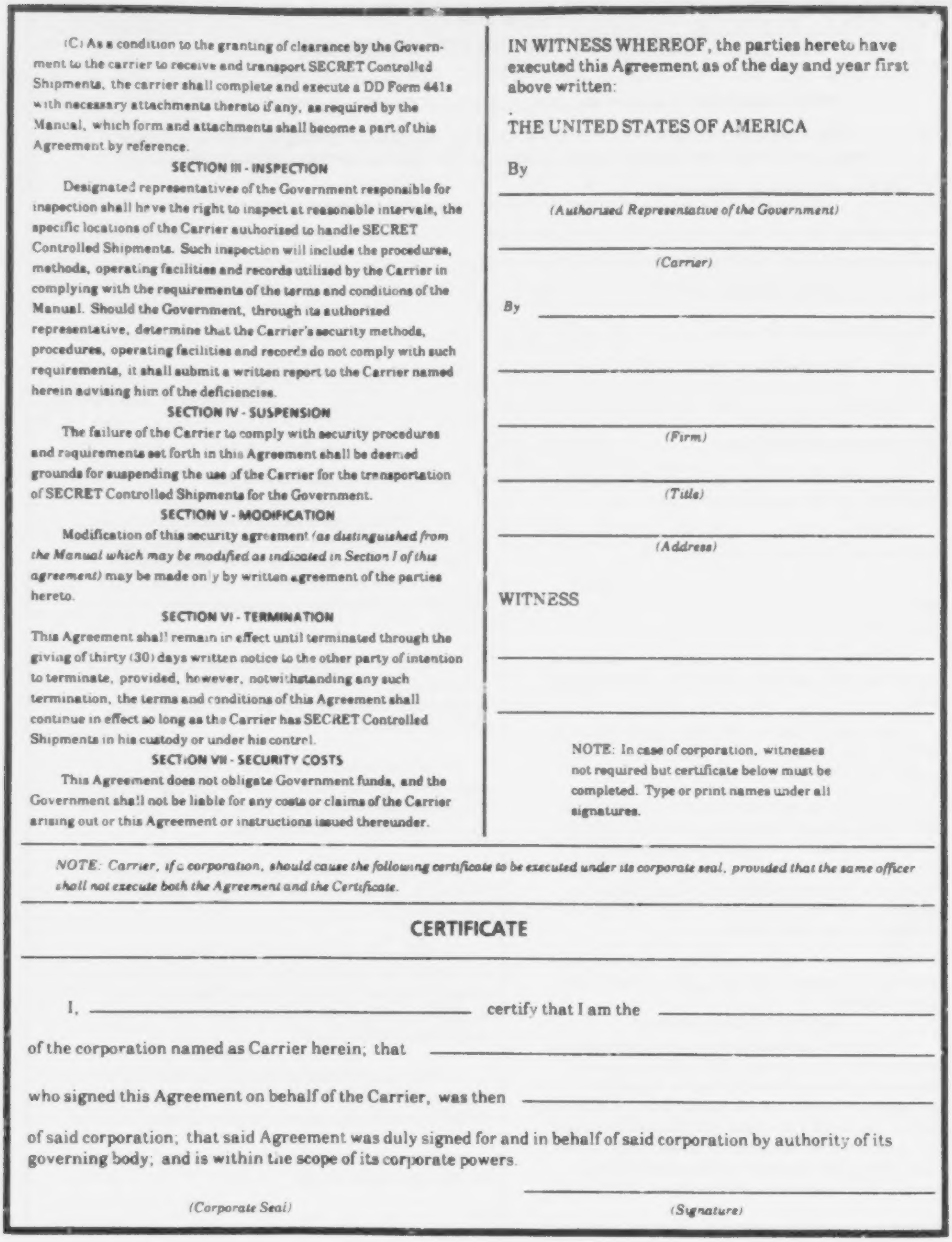
(Continue on reverse side)

DIS Form 1149, Dec 87 Replaces DIS Form 1149, May 83 which is obsolete.

SAMPLE

DIS Form 1149

Page Two



(C) As a condition to the granting of clearance by the Government to the carrier to receive and transport SECRET Controlled Shipments, the carrier shall complete and execute a DD Form 441s with necessary attachments thereto if any, as required by the Manual, which form and attachments shall become a part of this Agreement by reference.

SECTION III - INSPECTION

Designated representatives of the Government responsible for inspection shall have the right to inspect at reasonable intervals, the specific locations of the Carrier authorized to handle SECRET Controlled Shipments. Such inspection will include the procedures, methods, operating facilities and records utilized by the Carrier in complying with the requirements of the terms and conditions of the Manual. Should the Government, through its authorized representative, determine that the Carrier's security methods, procedures, operating facilities and records do not comply with such requirements, it shall submit a written report to the Carrier named herein advising him of the deficiencies.

SECTION IV - SUSPENSION

The failure of the Carrier to comply with security procedures and requirements set forth in this Agreement shall be deemed grounds for suspending the use of the Carrier for the transportation of SECRET Controlled Shipments for the Government.

SECTION V - MODIFICATION

Modification of this security agreement *(as distinguished from the Manual which may be modified as indicated in Section I of this agreement)* may be made only by written agreement of the parties hereto.

SECTION VI - TERMINATION

This Agreement shall remain in effect until terminated through the giving of thirty (30) days written notice to the other party of intention to terminate, provided, however, notwithstanding any such termination, the terms and conditions of this Agreement shall continue in effect so long as the Carrier has SECRET Controlled Shipments in his custody or under his control.

SECTION VII - SECURITY COSTS

This Agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Carrier arising out of this Agreement or instructions issued thereunder.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first above written:

THE UNITED STATES OF AMERICA

By ______________________________

(Authorized Representative of the Government)

____

(Carrier)

By ______________________________

____

____

(Firm)

____

(Title)

____

(Address)

WITNESS

____

____

NOTE: In case of corporation, witnesses not required but certificate below must be completed. Type or print names under all signatures.

NOTE: Carrier, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, ______________________________ certify that I am the ______________________________

of the corporation named as Carrier herein; that ______________________________

who signed this Agreement on behalf of the Carrier, was then ______________________________

of said corporation; that said Agreement was duly signed for and in behalf of said corporation by authority of its governing body; and is within the scope of its corporate powers.

(Corporate Seal)

____

(Signature)

best copy available

SAMPLE

DIS Form 1150

APPENDAGE TO DEPARTMENT OF DEFENSE TRANSPORTATION SECURITY AGREEMENT	FORM APPROVED OMB NO 0704-0198 EXP DATE APR 10 1990

It is further agreed, on this _____ day of _________ 19__, by and between the United States of America through the Defense Investigative Service acting for the Department of Defense, hereinafter called the Government, and _____________________, which has entered into the Transportation Security Agreement to which this appendage is made a part that the terminals listed below, owned and/or operated by said carrier are included in and covered by the provisions of the said Transportation Security Agreement, and Certificate Pertaining to Foreign Affiliation, DD Form 441s. It is further agreed that the terminals listed below are the only ones which will be used for the traesportation of SECRET Shipments.

NAME OF TERMINAL	NUMBER AND STREET ADDRESS	CITY AND STATE

CARRIER	TITLE
BY *(Authorized Representative of Carrier)*	ADDRESS

DIS Form 1150, Dec 87 Replaces DIS Form 1150, Sep 86, which is obsolete.

THIS PAGE IS BLANK . . .

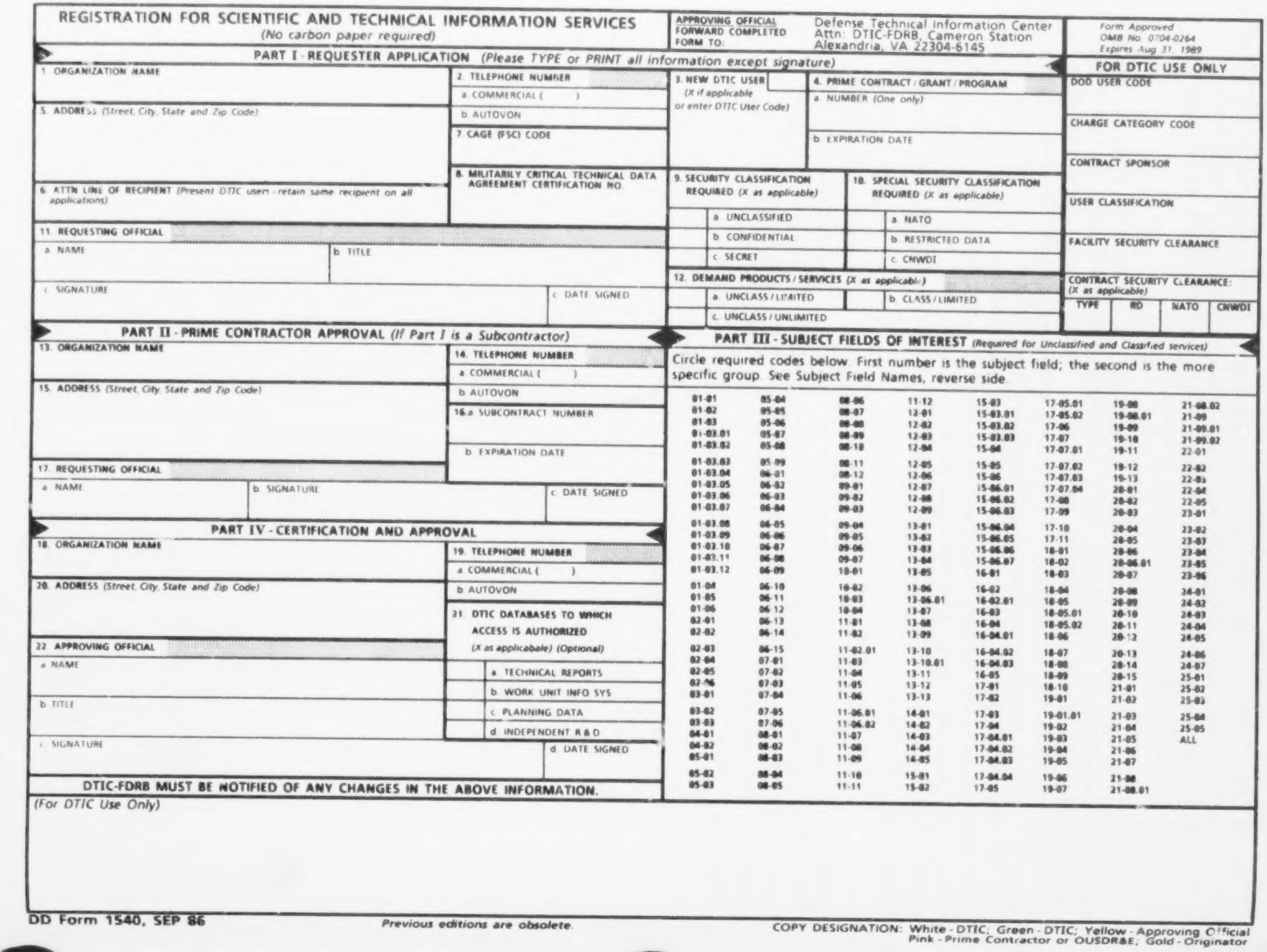
U. "Facility Clearance Register" (DD Form 1541) and "Registration for Scientific and Technical Information Services" (DD Form 1540). The purpose of the DD Form 1541 is to provide for uniform certification of a facility's security clearance and safeguarding ability to the Defense Technical Information Center (DTIC) and to provide notice of changes affecting an existing certification.

1. For initial certifications, part I of the DD Form 1541 is executed by the contractor in accordance with instructions appearing on the form. It is forwarded in duplicate to the CSO. That office shall complete part II of the form, noting in the "Remarks" section any limitations on the facility's eligibility to receive and store classified material. The original form, when certified, shall be forwarded to the DTIC. Contractors shall submit the DD Form 1541 only when requesting approval of the first DD Form 1540. When certified, the DD Form 1541 remains in effect for all future registrations or until changes occur affecting the clearance or safeguarding ability of the certified facility.

2. A copy of DD Form 1540 is included for information purposes. It is used to become eligible for the services of DTIC. The completed form is forwarded to the appropriate contracting officer. That office shall complete Part IV of the form and forward it to DTIC. Additional copies may be obtained from the following: DTIC, ATTN: DTIC-FDRB, Cameron Station, Alexandria, Virginia 22304-6145.

SAMPLE

DD Form 1540



REGISTRATION FOR SCIENTIFIC AND TECHNICAL INFORMATION SERVICES
(No carbon paper required)

APPROVING OFFICIAL FORWARD COMPLETED FORM TO:
Defense Technical Information Center
Attn: DTIC-FDRB, Cameron Station
Alexandria, VA 22304-6145

Form Approved
OMB No. 0704-0264
Expires Aug 31, 1989

PART I - REQUESTER APPLICATION *(Please TYPE or PRINT all information except signature)*

1. ORGANIZATION NAME
2. TELEPHONE NUMBER
a. COMMERCIAL (   )
b. AUTOVON
3. NEW DTIC USER ☐ *(X if applicable or enter DTIC User Code)*
4. PRIME CONTRACT / GRANT / PROGRAM
a. NUMBER *(One only)*
b. EXPIRATION DATE
5. ADDRESS *(Street, City, State and Zip Code)*
6. ATTN LINE OF RECIPIENT *(Present DTIC users - retain same recipient on all applications)*
7. CAGE (FSC) CODE
8. MILITARILY CRITICAL TECHNICAL DATA AGREEMENT CERTIFICATION NO.
9. SECURITY CLASSIFICATION REQUIRED *(X as applicable)*
☐ a. UNCLASSIFIED
☐ b. CONFIDENTIAL
☐ c. SECRET
10. SPECIAL SECURITY CLASSIFICATION REQUIRED *(X as applicable)*
☐ a. NATO
☐ b. RESTRICTED DATA
☐ c. CNWDI
11. REQUESTING OFFICIAL
a. NAME
b. TITLE
c. SIGNATURE
c. DATE SIGNED
12. DEMAND PRODUCTS / SERVICES *(X as applicable)*
☐ a. UNCLASS / LIMITED
☐ b. CLASS / LIMITED
☐ c. UNCLASS / UNLIMITED

FOR DTIC USE ONLY

DOD USER CODE
CHARGE CATEGORY CODE
CONTRACT SPONSOR
USER CLASSIFICATION
FACILITY SECURITY CLEARANCE
CONTRACT SECURITY CLEARANCE: *(X as applicable)*

TYPE	RD	NATO	CNWDI

PART II - PRIME CONTRACTOR APPROVAL *(If Part I is a Subcontractor)*

13. ORGANIZATION NAME
14. TELEPHONE NUMBER
a. COMMERCIAL (   )
b. AUTOVON
15. ADDRESS *(Street, City, State and Zip Code)*
16.a SUBCONTRACT NUMBER
b. EXPIRATION DATE
17. REQUESTING OFFICIAL
a. NAME
b. SIGNATURE
c. DATE SIGNED

PART III - SUBJECT FIELDS OF INTEREST *(Required for Unclassified and Classified services)*

Circle required codes below. First number is the subject field; the second is the more specific group. See Subject Field Names, reverse side.

01-01
01-02
01-03
01-03.01
01-03.02
01-03.03
01-03.04
01-03.05
01-03.06
01-03.07
01-03.08
01-03.09
01-03.10
01-03.11
01-03.12
01-04
01-05
01-06
02-01
02-02
02-03
02-04
02-05
02-06
03-01
03-02
03-03
04-01
04-02
05-01
05-02
05-03

05-04
05-05
05-06
05-07
05-08
05-09
06-01
06-02
06-03
06-04
06-05
06-06
06-07
06-08
06-09
06-10
06-11
06-12
06-13
06-14
06-15
07-01
07-02
07-03
07-04
07-05
07-06
08-01
08-02
08-03
08-04
08-05

08-06
08-07
08-08
08-09
08-10
08-11
08-12
09-01
09-02
09-03
09-04
09-05
09-06
09-07
10-01
10-02
10-03
10-04
11-01
11-02
11-02.01
11-03
11-04
11-05
11-06
11-06.01
11-06.02
11-07
11-08
11-09
11-10
11-11

11-12
12-01
12-02
12-03
12-04
12-05
12-06
12-07
12-08
12-09
13-01
13-02
13-03
13-04
13-05
13-06
13-06.01
13-07
13-08
13-09
13-10
13-10.01
13-11
13-12
13-13
14-01
14-02
14-03
14-04
14-05
15-01
15-02

15-03
15-03.01
15-03.02
15-03.03
15-04
15-05
15-06
15-06.01
15-06.02
15-06.03
15-06.04
15-06.05
15-06.06
15-06.07
16-01
16-02
16-02.01
16-03
16-04
16-04.01
16-04.02
16-04.03
16-05
17-01
17-02
17-03
17-04
17-04.01
17-04.02
17-04.03
17-04.04
17-05

17-05.01
17-05.02
17-06
17-07
17-07.01
17-07.02
17-07.03
17-07.04
17-08
17-09
17-10
17-11
18-01
18-02
18-03
18-04
18-05
18-05.01
18-05.02
18-06
18-07
18-08
18-09
18-10
19-01
19-01.01
19-02
19-03
19-04
19-05
19-06
19-07

19-08
19-08.01
19-09
19-10
19-11
19-12
19-13
20-01
20-02
20-03
20-04
20-05
20-06
20-06.01
20-07
20-08
20-09
20-10
20-11
20-12
20-13
20-14
20-15
21-01
21-02
21-03
21-04
21-05
21-06
21-07
21-08
21-08.01

21-08.02
21-09
21-09.01
21-09.02
22-01
22-02
22-03
22-04
22-05
23-01
23-02
23-03
23-04
23-05
23-06
24-01
24-02
24-03
24-04
24-05
24-06
24-07
25-01
25-02
25-03
25-04
25-05
ALL

PART IV - CERTIFICATION AND APPROVAL

18. ORGANIZATION NAME
19. TELEPHONE NUMBER
a. COMMERCIAL (   )
b. AUTOVON
20. ADDRESS *(Street, City, State and Zip Code)*
21. DTIC DATABASES TO WHICH ACCESS IS AUTHORIZED *(X as applicabale) (Optional)*
☐ a. TECHNICAL REPORTS
☐ b. WORK UNIT INFO SYS
☐ c. PLANNING DATA
☐ d. INDEPENDENT R&D
22. APPROVING OFFICIAL
a. NAME
b. TITLE
c. SIGNATURE
d. DATE SIGNED

DTIC-FDRB MUST BE NOTIFIED OF ANY CHANGES IN THE ABOVE INFORMATION.

(For DTIC Use Only)

DD Form 1540, SEP 86 *Previous editions are obsolete.*

COPY DESIGNATION: White - DTIC; Green - DTIC; Yellow - Approving Official
Pink - Prime Contractor or OUSDR&E; Gold - Originator

SAMPLE

DD Form 1540

SUBJECT FIELD AND GROUP STRUCTURE

01	AVIATION TECHNOLOGY
01	Aerodynamics
02	Military Aircraft Operations
03	Aircraft
03.01	Helicopters
03.02	Bombers
03.03	Attack and Fighter Aircraft
03.04	Patrol and Reconnaissance Aircraft
03.05	Transport Aircraft
03.06	Training Aircraft
03.07	V/STOL
03.08	Gliders and Parachutes
03.09	Civilian Aircraft
03.10	Pilotless Aircraft
03.11	Lighter-than-Air Aircraft
03.12	Research and Experimental Aircraft
04	Flight Control and Instrumentation
05	Terminal Flight Facilities
06	Commercial and General Aviation

02	AGRICULTURE
01	Agricultural Chemistry
02	Agricultural Economics
03	Agricultural Engineering
04	Agronomy, Horticulture and Aquiculture
05	Animal Husbandry and Veterinary Medicine
06	Forestry

03	ASTRONOMY AND ASTROPHYSICS
01	Astronomy
02	Astrophysics
03	Celestial Mechanics

04	ATMOSPHERIC SCIENCES
01	Atmospheric Physics
02	Meteorology

05	BEHAVIORAL AND SOCIAL SCIENCES
01	Administration and Management
02	Information Science
03	Economics and Cost Analysis
04	Government and Political Science
05	Sociology and Law
06	Humanities and History
07	Linguistics
08	Psychology
09	Personnel Management and Labor Relations

06	BIOLOGICAL AND MEDICAL SCIENCES
01	Biochemistry
02	Genetic Engineering and Molecular Biology
03	Biology
04	Anatomy and Physiology
05	Medicine and Medical Research
06	Ecology
07	Radiobiology
08	Food, Food Service and Nutrition
09	Hygiene and Sanitation
10	Stress Physiology
11	Toxicology
12	Medical Facilities, Equipment and Supplies
13	Microbiology
14	Weapons Effects (Biological)
15	Pharmacology

07	CHEMISTRY
01	Industrial Chemistry and Chemical Processing
02	Inorganic Chemistry
03	Organic Chemistry
04	Physical Chemistry
05	Radiation and Nuclear Chemistry
06	Polymer Chemistry

08	EARTH SCIENCES AND OCEANOGRAPHY
01	Biological Oceanography
02	Cartography and Aerial Photography
03	Physical and Dynamic Oceanography
04	Geomagnetism
05	Geodesy
06	Geography
07	Geology, Geochemistry and Mineralogy
08	Hydrology, Limnology and Potamology
09	Mining Engineering
10	Soil Mechanics
11	Seismology
12	Snow, Ice and Permafrost

09	ELECTROTECHNOLOGY AND FLUIDICS
01	Electrical and Electronic Equipment
02	Fluidics and Fluerics
03	Lasers and Masers
04	Line, Surface and Bulk Acoustic Wave Devices
05	Electrooptical and Optoelectronic Devices
06	Acoustooptic and Optoacoustic Devices
07	Electromagnetic Shielding

10	POWER PROPULSION AND ENERGY CONVERSION (Nonpropulsive)
01	Non-Electrical Energy Conversion
02	Electric Power Production and Distribution
03	Electrochemical Energy Storage
04	Energy Storage

11	MATERIALS
01	Adhesives, Seals and Binders
02	Ceramics, Refractories and Glass
02.01	Refractory Fibers
03	Coatings, Colorants and Finishes
04	Laminates and Composite Materials
05	Textiles
06	Metallurgy and Metallography
06.01	Properties of Metals and Alloys
06.02	Fabrication Metallurgy
07	Miscellaneous Materials
08	Lubricants and Hydraulic Fluids
09	Plastics
10	Elastomers and Rubber
11	Solvents, Cleaners and Abrasives
12	Wood, Paper and Related Forestry Products

12	MATHEMATICAL AND COMPUTER SCIENCES
01	Numerical Mathematics
02	Theoretical Mathematics
03	Statistics and Probability
04	Operations Research
05	Computer Programming and Software
06	Computer Hardware
07	Computer Systems
08	Computer Systems Management and Standards
09	Cybernetics

13	MECHANICAL, INDUSTRIAL, CIVIL AND MARINE ENGINEERING
01	Air Conditioning, Heating, Lighting and Ventilating
02	Civil Engineering
03	Construction Equipment, Materials and Supplies
04	Containers and Packaging
05	Couplers, Fasteners and Joints
06	Surface Transportation and Equipment
06.01	Surface Effect Vehicles and Amphibious Vehicles
07	Hydraulic and Pneumatic Equipment
08	Manufacturing and Industrial Engineering and Control of Production Systems
09	Machinery and Tools
10	Marine Engineering
10.01	Submarine Engineering
11	Pumps, Filters, Pipes, Tubing, Fittings and Valves
12	Safety Engineering
13	Structural Engineering and Building Technology

14	TEST EQUIPMENT, RESEARCH FACILITIES AND REPROGRAPHY
01	Holography
02	Test Facilities, Equipment and Methods
03	Recording and Playback Devices
04	Photography
05	Printing and Graphic Arts

15	MILITARY SCIENCES
01	Military Forces and Organizations
02	Civil Defense
03	Defense Systems
03.01	Antimissile Defense Systems
03.02	Antiaircraft Defense Systems
03.03	Antisatellite Defense Systems
04	Military Intelligence
05	Logistics, Military Facilities and Supplies
06	Military Operations, Strategy and Tactics
06.01	Naval Surface Warfare
06.02	Undersea and Antisubmarine Warfare
06.03	Chemical, Biological and Radiological Warfare
06.04	Nuclear Warfare
06.05	Space Warfare
06.06	Land Mine Warfare
06.07	Unconventional Warfare

16	GUIDED MISSILE TECHNOLOGY
01	Guided Missile Launching and Basing Support
02	Guided Missile Trajectories, Accuracy and Ballistics
02.01	Guided Missile Dynamics, Configurations and Control Surfaces
03	Guided Missile Warheads and Fuzes
04	Guided Missiles
04.01	Air- and Space-Launched Guided Missiles
04.02	Surface-Launched Guided Missiles
04.03	Underwater-Launched Guided Missiles
05	Guided Missile Reentry Vehicles

17	NAVIGATION, DETECTION AND COUNTERMEASURES
01	Acoustic Detection and Detectors
02	Non-Acoustic and Non-Magnetic Submarine Detection
03	Direction Finding
04	Countermeasures
04.01	Radio Countermeasures
04.02	Acoustic Countermeasures
04.03	Radar Countermeasures
04.04	Optical Countermeasures
05	Optical Detection and Detectors
05.01	Infrared Detection and Detectors
05.02	Ultraviolet Detection and Detectors
06	Magnetic and Electric Field Detection and Detectors
07	Navigation and Guidance
07.01	Land and Riverine Navigation and Guidance
07.02	Underwater and Marine Navigation and Guidance
07.03	Air Navigation and Guidance
07.04	Space Navigation and Guidance
08	Miscellaneous Detection and Detectors
09	Active and Passive Radar Detection and Equipment
10	Seismic Detection and Detectors
11	Target Direction, Range and Position Finding

18	NUCLEAR SCIENCE AND TECHNOLOGY
01	Fusion Devices (Thermonuclear)
02	Isotopes
03	Nuclear Explosions and Devices (Non-Military)
04	Nuclear Instrumentation
05	Nuclear Power Plants and Fission Reactor Engineering
05.01	Nuclear Fission Reactors (Power)
05.02	Nuclear Fission Reactors (Non-Power)
06	Nuclear Radiation Shielding, Protection and Safety
07	Radioactivity, Radioactive Wastes and Fission Products
08	SNAP (Systems for Nuclear Auxiliary Power) Technology
09	Fission Reactor Physics
10	Fission Reactor Materials

19	ORDNANCE
01	Ammunition and Explosives
01.01	Pyrotechnics
02	Aerial Bombs
03	Combat Vehicles
04	Armor
05	Fire Control and Bombing Systems
06	Guns
07	Rockets
08	Underwater Ordnance
08.01	Torpedoes
09	Explosions
10	Ballistics
11	Nuclear Weapons
12	Directed Energy Weapons
13	Guided Munitions

20	PHYSICS
01	Acoustics
02	Crystallography
03	Electricity and Magnetism
04	Fluid Mechanics
05	Atomic and Molecular Physics and Spectroscopy
06	Optics
06.01	Fiber Optics and Integrated Optics
07	Particle Accelerators
08	Nuclear Physics and Elementary Particle Physics
09	Plasma Physics and Magnetohydrodynamics
10	Quantum Theory and Relativity
11	Mechanics
12	Solid State Physics
13	Thermodynamics
14	Radiofrequency Wave Propagation
15	Electromagnetic Pulses

21	PROPULSION, ENGINES AND FUELS
01	Air Breathing Engines (Unconventional)
02	Combustion and Ignition
03	Electric and Ion Propulsion
04	Fuels
05	Jet and Gas Turbine Engines
06	Nuclear Propulsion
07	Reciprocating and Rotating Engines
08	Rocket Engines
08.01	Liquid Propellant Rocket Engines
08.02	Solid Propellant Rocket Engines
09	Rocket Propellants
09.01	Liquid Rocket Propellants
09.02	Solid Rocket Propellants

22	SPACE TECHNOLOGY
01	Astronautics
02	Unmanned Spacecraft
03	Spacecraft Trajectories and Reentry
04	Ground Support Systems and Facilities for Space Vehicles
05	Manned Spacecraft

23	BIOTECHNOLOGY
01	Biomedical Instrumentation and Bioengineering
02	Human Factors Engineering and Man Machine Systems
03	Bionics
04	Protective Equipment
05	Life Support Systems
06	Escape, Rescue and Survival

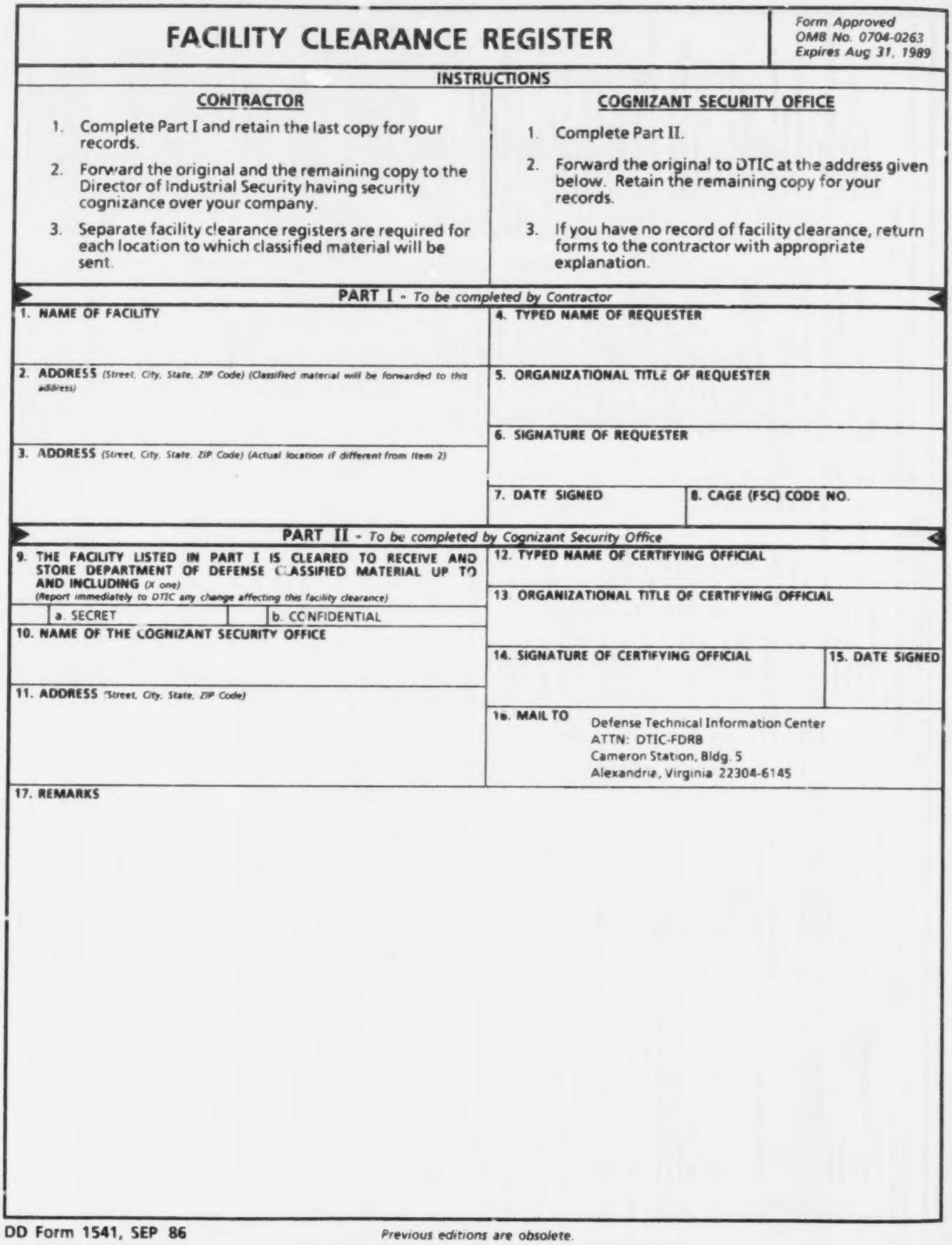
24	ENVIRONMENTAL POLLUTION AND CONTROL
01	Air Pollution and Control
02	Noise Pollution and Control
03	Solid Wastes Pollution and Control
04	Water Pollution and Control
05	Pesticides Pollution and Control
06	Radiation Pollution and Control
07	Environmental Health and Safety

25	COMMUNICATIONS
01	Telemetry
02	Radio Communications
03	Non-Radio Communications
04	Voice Communications
05	Command, Control and Communications Systems

DD Form 1540 Reverse, SEP 86

SAMPLE

DD Form 1541



FACILITY CLEARANCE REGISTER

Form Approved
OMB No. 0704-0263
Expires Aug 31, 1989

INSTRUCTIONS

CONTRACTOR	COGNIZANT SECURITY OFFICE
1. Complete Part I and retain the last copy for your records.	1. Complete Part II.
2. Forward the original and the remaining copy to the Director of Industrial Security having security cognizance over your company.	2. Forward the original to DTIC at the address given below. Retain the remaining copy for your records.
3. Separate facility clearance registers are required for each location to which classified material will be sent.	3. If you have no record of facility clearance, return forms to the contractor with appropriate explanation.

PART I - *To be completed by Contractor*

1. NAME OF FACILITY	4. TYPED NAME OF REQUESTER	
2. ADDRESS *(Street, City, State, ZIP Code) (Classified material will be forwarded to this address)*	5. ORGANIZATIONAL TITLE OF REQUESTER	
	6. SIGNATURE OF REQUESTER	
3. ADDRESS *(Street, City, State, ZIP Code) (Actual location if different from item 2)*	7. DATE SIGNED	8. CAGE (FSC) CODE NO.

PART II - *To be completed by Cognizant Security Office*

9. THE FACILITY LISTED IN PART I IS CLEARED TO RECEIVE AND STORE DEPARTMENT OF DEFENSE CLASSIFIED MATERIAL UP TO AND INCLUDING *(X one)* *(Report immediately to DTIC any change affecting this facility clearance)* ☐ a. SECRET ☐ b. CONFIDENTIAL	12. TYPED NAME OF CERTIFYING OFFICIAL	
	13. ORGANIZATIONAL TITLE OF CERTIFYING OFFICIAL	
10. NAME OF THE COGNIZANT SECURITY OFFICE	14. SIGNATURE OF CERTIFYING OFFICIAL	15. DATE SIGNED
11. ADDRESS *(Street, City, State, ZIP Code)*	16. MAIL TO Defense Technical Information Center ATTN: DTIC-FDRB Cameron Station, Bldg. 5 Alexandria, Virginia 22304-6145	

17. REMARKS

DD Form 1541, SEP 86 *Previous editions are obsolete.*

V. Letter Agreement to Safeguard Classified Information for an Employee Performing Consultant Services. ("TYPE C" CONSULTANT). This agreement shall be prepared and executed by a contractor if the contractor agrees to accept responsibility for safeguarding classified information released to an employee furnishing consultant services.

The contractor shall send the original to the CSO and distribute copies as indicated on the agreement. In case of failure to execute this agreement, the consultant shall be cleared as a facility.

SAMPLE

(Sample)
"TYPE C" CONSULTANT AGREEMENT
(Company Letterhead)

To: ______________________ ______________________
(cognizant security office) (date)

Dear ______________________:

In accordance with paragraph 70 of the "Industrial Security Manual for Safeguarding Classified Information" (ISM), the ______________________ (name of cleared facility) cleared to the level of ______________________ (level of facility clearance) and ______________________ (name of employee) an employee cleared for access to ______________ (level) classified information, by ______________________ (activity granting clearance) on ______________ (date) who is serving as a consultant to ______________________ (name of using facility or user agency activity) hereby jointly agree to the following.

(i) Place classified material received and/or produced by said employee in his or her capacity as a consultant into the facility's classified material control system.

(ii) Provide the employee with an approved container in which to store classified material relating to his or her consulting activity.

(iii) Incorporate the facility's standard practice procedures implementing the access limitation requirements of paragraphs 70a(2) and 70a(3), ISM.

(iv) Abide by the facility's standard practice procedures in handling classified material relating to the employee's consulting activity.

(v) Advise the cognizant security office and either the contractor or the user agency activity to which the employee is a consultant of any change in the consultant's status as an employee of the facility.

______________________ ______________________
(date) (employing contractor signature)

____
(title)

______________________ ______________________
(date) (employee-consultant signature)

Copy to:
Facility of Employee Consultant
Contractor or User Agency to which Employee is Consultant
Employee Consultant

Appendix II. DERIVATIVE CLASSIFICATION INFORMATION AND PROCEDURES

A. Scope and Application.

1. General. E.O. 12356 prescribes a uniform system for classifying and declassifying national security information. The E.O. recognizes that it is essential that the public be informed concerning the activities of its government, but that the interests of the U.S. and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information classified under E.O. 12356 and prior orders shall be declassified or downgraded as soon as national security considerations permit. Information is declassified based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event that permits declassification. Information that continues to meet the classification criteria, despite the passage of time, will remain classified and continue to be protected.

2. User Agency Information. In compliance with their responsibilities under the above E.O., the Secretaries of Defense, Commerce, State, Treasury, Transportation, Interior, Agriculture, and Labor; the Attorney General, Department of Justice; the Comptroller General of the United States, General Accounting Office; the Chairman, Board of Governors, Federal Reserve System; the Administrators, General Services Administration, Small Business Administration, National Aeronautics and Space Administration, and Environmental Protection Agency; and the Directors, National Science Foundation, U.S. Arms Control and Disarmament Agency, Federal Emergency Management Agency, United States Information Agency and the United States Trade Representative (all hereinafter referred to as UA's) * have prescribed that the provisions of this appendix shall apply to all classified information originated in the UA's or by one of their components or contractors. This encompasses all classified information originated by: the OSD and DoD agencies; the present and former Joint Chiefs of Staff and Joint Staff; the Department of Army and former War Department; the Department of Navy; the Department of Air Force and former Army Air Forces; the U.S. Coast Guard, when acting as a part of Navy, Treasury, or Transportation; NASA and predecessor NASA agencies, including the National Advisory Committee for Aeronautics; the FAA, prior and subsequent to its assignment to the Department of Transportation, predecessor FAA agencies, including the Civil Aeronautics Administration and the Airways Modernization Board, formerly of the Department of Commerce; joint committees or agencies comprised entirely of representatives from within the above described agencies or their predecessor agencies; other U.S. Government agencies whose functions have officially transferred to any of the above agencies; and contractors in the performance of contracts awarded by or on behalf of the UA's, their components, or their predecessors.

3. Authority of Contractors. The contractor shall apply and implement the provisions of this appendix, unless otherwise instructed by his or her

contracting officer 1/. In those cases in which a contracting officer determines that the material has been improperly designated, the contracting officer shall instruct the contractor to mark the material to reflect the correct designation.

4. Responsibility of Contractors. Each contractor who possesses classified material affected by this appendix is responsible for initiating action to apply the appropriate notation and to change or cancel classifications as prescribed herein. Such actions are the responsibility of each holder of classified material; they constitute an implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of classification 2/. Pending the re-marking of classified material, as prescribed in this appendix, the contractor shall safeguard the material in accordance with the classification marked on it.

5. Requests for Advice. When the contractor cannot determine exactly which provision of this appendix applies to certain classified information or material, they shall request advice from the contracting officer concerned. If the contracting officer is unknown, such requests will be forwarded through UA contracting channels, as appropriate. If the channels are not known, the request will be sent directly to the appropriate office shown below. All such requests must include a complete description or identification of the classified information or document in question.

a. Army. Department of Army, ATTN: DAMI-CIS, Room 2D481, The Pentagon, Washington, DC 20310-1051

b. Navy. Department of Navy, Chief of Naval Operations, OP-09N, Washington, DC 20350-2000

c. Air Force. Department of Air Force, HQ Chief, Industrial Security Branch, Air Force Office of Security Police, Kirtland AFB, NM 87117-6001

d. NASA. Headquarters, NASA, Security Office, ATTN: NIS, 400 Maryland Avenue, SW, Washington, DC 20546

e. Commerce. Department of Commerce, Director, Office of Security, ATTN: H5044 OSY, 14th Street and Constitution Avenue, NW, Washington, DC 20230

1/ In those cases in which a contractor receives instructions that appear to be in conflict with the provisions of this appendix, the contractor shall immediately notify the contracting officer of the conflicting instructions. Pending resolution of the problem, he or she shall comply with the most recent instructions received from the contracting officer.

2/ The date of the initial specification, drawing, or blueprint from which hardware is manufactured may be used as the date from which to compute automatic downgrading or declassification of the information, which may be disclosed by the hardware.

f. GSA. General Services Administration, Director of Audit Resolution and Internal Controls, Office of Administration, 18th and F Streets, NW, (Room 5001), Washington, DC 20405

g. State. Department of State, Bureau of Diplomatic Security, ATTN: DS/PRD/IN, 2201 C Street, NW, Washington, DC 20520

h. SBA. Small Business Administration, Security Officer, Office of Operational Support of Security, 1441 L Street, NW, Washington, DC 20416

i. NSF. National Science Foundation, Division of Personnel and Management, Chief, Personnel Administration Branch/Security Officer, 1800 G Street, NW, (Room 208), Washington, DC 20550

j. Treasury. Department of Treasury, Director, (Office of Security), Room 1302, Main Treasury Building, 1500 Pennsylvania Avenue, NW, Washington DC 20220

k. Transportation. Department of Transportation, Office of Security, Chief, Personnel and Information Security Division, M-73, Room 7402, 400 Seventh Street, SW, Washington, DC 20590

l. Interior. Department of the Interior, Chief, Division of Enforcement and Security Management, 18th and C Streets, NW, (Room 5426), Washington, DC 20240

m. Agriculture. Department of Agriculture, Security, Employee and Labor Relations Staff, (SELRS), Office of Personnel, Room 16W, Administration Building, 14th and Independence Avenue, SW, Washington, DC 20250

n. USIA. U.S. Information Agency, Chief, Domestic Operations Division, Washington, DC 20547

o. Labor. Department of Labor, Information Security Staff, Room S1524, 200 Constitution Avenue NW, Washington, DC 20210

p. EPA. Environmental Protection Agency, Director, Security and Property Management Branch, PM-215, 401 M Street, SW, Washington, DC 20460

q. FRS. Federal Reserve System, Chief of Security, Division of Support Services, Board of Governors, 20th and C Streets, NW, Washington, DC 20551

r. Justice. Department of Justice, Chief, Special Security Center, Ninth and Constitution Avenue, NW, (Room 6744), Washington, DC 20530

s. ACDA. U.S. Arms Control and Disarmament Agency, Director of Security, 320 21st Street, NW, Room 5933, Washington, D.C. 20451

t. FEMA. Federal Emergency Management Agency, Director, Office of Security, (Room 128), 500 C Street, SW, Washington, DC 20472

u. GAO. General Accounting Office, Director, Office of Security & Safety, 441 G Street, NW, Room 4844, Washington, DC 20548

v. USTR. Director, Administrative Services, Office of the United States Trade Representatives, Executive Office of the President, Washington, DC 20506

w. If the contractor is unable to obtain advice from the UA's listed above, assistance may be requested from the Deputy Under Secretary of Defense for Policy, ATTN: Director, Information Security, The Pentagon, Washington, D.C. 20301.

B. Downgrading/Declassification and "Classified by" Line Procedures.

1. General. All derivatively classified material shall be marked to reflect declassification instructions, the source of classification (shown on the "Classified by" line), and, if applicable, downgrading instructions. Documents shall show the required information either on the cover, first page, title page, or in a similarly prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation.

The markings used to show this information shall be as follows:

CLASSIFIED BY ____________________ (Required)
DOWNGRADE TO ______________ ON ______________ (As Appropriate)
DECLASSIFY ON ______________________________ (Required)

a. On electronically transmitted messages, the "classified by" line is not required; the other markings are required and may be included on the last line of text and may be abbreviated as follows:

DNG/"S" or "C"/ (date or event)
DECL ____________________

b. Material containing RESTRICTED DATA may only be declassified by the DOE. FORMERLY RESTRICTED DATA may only be declassified on a joint determination by the DoD and the DOE. Therefore, only a "Classified by" line is shown on the material. The "Declassify on" line is not to be used.

2. The "Classified by" line.

a. In completing the "Classified by" line, the contractor shall identify the applicable DD Form 254 (see paragraph b below) or other UA guidance. In addition, if any single guidance source other than, or supplemental to, the applicable DD Form 254 is followed, that source will also be shown in such a way that, standing alone, it will be sufficiently complete to identify it, including its date. If two or more guidance sources other than or in addition to the applicable DD Form 254 are followed, the identification of the DD Form 254 will be followed by the phrase "multiple sources" (for example, DD Form 254, August 30, 1982, RFQ #12345, Multiple Sources). In each such case, when the phrase "multiple sources" is used, the contractor shall maintain adequate records to support the application of the classification marking and shall retain such records for the duration of the contract or program under which the document was created. The records could take the form of a bibliography identifying the applicable classification sources and be included in the text.

b. Identification of the applicable DD Form 254 in the "Classified by" line will always include at least the following:

(1) the date of the DD Form 254, and

(2) the specific designator (for example, contract number) of the contract or other requirements document for which the DD Form 254 was issued 3/.

3. The "Declassify on" Line. In completing the "Declassify on" line, the contractor shall use the information specified in or with the DD Form 254 provided by a UA or cite the source document.

4. The "Downgrade to" Line. In completing the "Downgrade to" line, the contractor shall insert SECRET or CONFIDENTIAL and an effective date or event as indicated in or with the DD Form 254, or cite the source document.

C. Applying Derivative Markings to New Material.

1. Pre-August 1, 1982. New material that derives its classification from material classified or issued prior to August 1, 1982 shall be treated as follows:

a. If the DD Form 254 or source material bears a date or event for declassification, that date or event shall be applied to the new material.

b. If the DD Form 254 or source material bears no date or event for declassification, bears an indefinite date or event, or is marked for declassification review, the new material shall be marked with the notation: "Originating Agency's Determination Required" or "OADR."

2. After August 1, 1982. New material that derives its classification from a DD Form 254 or source material bearing a date on or after August 1, 1982 shall be marked with the declassification date or event, or with the notation, "Originating Agency's Determination Required," or "OADR" as specified in the DD Form 254 or source material.

D. Most Restrictive Marking Determination. In all cases where a new document or material is classified based on "multiple sources," the most remote date or event for declassification shown on any source shall be assigned to the new document or material. If any source shows the notation "Originating Agency's Determination Required" or "OADR," the new document or material shall also be assigned this notation. For example, if one source indicates declassification on December 31, 1988 and another source indicates, "Originating Agency's Determination Required," or "OADR," the notation, "Originating Agency's Determination Required," or "OADR" shall be assigned to the new material, because it is the most restrictive marking.

3/ For potential prime contractors responding to an IFB, RFQ, or RFP, when no contract designator is shown in item 3a of the DD Form 254, the designator shown in item 3c of the DD Form 254 shall be used. Prime contractors and subcontractors at all tiers shall use the designator set forth in item 3a of the DD Form 254.

E. Downgrading/Declassification Actions for Pre-August 1, 1982 Material.

1. Documents and material classified under E.O. 12065, and predecessor E.O.'s that are marked for automatic downgrading or declassification on a specified date or event, may be downgraded and declassified pursuant to such markings. Such documents or material need not be re-marked, except in accordance with paragraph 11d. Information extracted from these documents or material for use in new documents or material shall be marked for declassification as specified in the source document.

2. Documents and material classified under E.O. 12065, and predecessor E.O.'s that are not marked for automatic downgrading or declassification on a specified date or event, shall not be downgraded or declassified without authorization of the originating agency. Such documents or material need not be re-marked. Information extracted from these documents or material for use in new documents or material shall be marked for declassification on the determination of the originating agency; that is, the "Declassify on" line shall be completed with the notation, "Originating Agency's Determination Required," or "OADR."

F. Extracts of Information. Information extracted from a classified source shall be derivatively classified or not classified, in accordance with the classification markings shown in the source. The overall and internal markings of the source should supply adequate classification guidance. If internal markings or classification guidance are not found in the source, and no reference is made to an applicable and available classification guide, the extracted information shall be classified according either to the overall marking of the source or the guidance obtained from the classifier of the source material.

G. Changing Classification Markings. At the time the material is actually downgraded or declassified, the action to change the classification markings shall be initiated and performed, in accordance with the provisions of paragraph 11. When classification markings are changed or canceled, an entry, when appropriate, shall be made in the control station records prescribed in paragraph 12, to reflect such change or cancellation.

H. Release of Declassified Information. Declassification, either automatically or by individual review and determination, is not automatically an approval for public disclosure. Accordingly, contractors shall request approval for public disclosure of "declassified" information, in accordance with the provisions of paragraph 5o.

Appendix III. FOREIGN CLASSIFIED CONTRACTS

Table Outlining Responsibilities for Security Actions.

Certain duties which this manual assigns to the contracting officer or to the contracting UA are, with respect to foreign classified contracts, assigned to the Deputy Director (Industrial Security), HQ DIS, the administrative contracting office, or the CSO.

Table I shows the assignment of these duties. Contractors will submit their requests for instructions or guidance as set forth below. Duties not specifically assigned herein are reserved to the foreign government agency or foreign contracting activity concerned. Requests for instructions in such cases shall be submitted through the Deputy Director (Industrial Security), HQ DIS.

Table 1

Action	References	Deputy Director (Industrial Security), HQ DIS	Admin-istrative Contracting Officer	Cognizant Security Office
1. Approves retention of classified information by contractor or subcontractor.	Pars. 51, 5m, and 64, ISM		X	
2. Authorizes and provides instruction for transmission of classified information outside the facility.	Pars. 5 and 17e, ISM		X	X
3. Authorizes reproduction of classified information.	Par. 18. ISM		X	
4. Authorizes destruction of certain classified information.	Par. 19, ISM		X	
5. Approves electrical alarm service.	Pars. 35 and 36, ISM		X 2/	X
6. Approves controlled area.	Par. 34, ISM		X 2/	X
7. Approves visits for Categories 2 and 3.	Par. 41, ISM		X 1/	
8. Authorizes disclosure of TOP SECRET information to subcontractor.	Par. 59, ISM		X	
9. Receives notification of award of classified subcontractor 3/.	Par. 62, ISM	X	X	X
10. a. Approves Security Classification Guidance for subcontracts.	Par. 60.ISM		X	
b. Obtains Security Classification Guidance for subcontracts.		X	X	

1/ Some foreign contracts will be managed by foreign personnel directly from the country concerned, the country's Washington embassy, or other means with no U.S. contracting officer involved. U.S. UA's control Category 4 type visits as well as Category 3. Necessary coordination will be effected with the Deputy Director (Industrial Security), HQ DIS, the CSO, and the contractor concerned.

2/ If costs are involved.

3/ This notice shall be sent to the CSO of the subcontractor.

Appendix IV. REQUIREMENTS FOR THE CONSTRUCTION OF STORAGE VAULTS AND STRONGROOMS

A. Application. This appendix specifies the minimum standards required for the construction of vaults and strongrooms used as storage facilities for classified material, in accordance with paragraph 14 of this manual. These standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing vaults or strongrooms. They will also be used for evaluating the adequacy of existing vaults and strongrooms.

B. Class A Vault.

1. Floor and Walls. The thickness of the floor and walls must be determined by structural requirements, but may not be less than 8-inch-thick reinforced concrete. Walls are to extend to the underside of the roof/ceiling slab above.

2. Roof/Ceiling. The roof or ceiling must be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less thick than the walls and floors.

3. Vault Door and Frame Unit. The vault door and frame unit shall be one that was originally procured from the FSS 1/.

4. Lock and Locking Parts. The lock shall conform to Underwriters' Standard No. 768 Group I-R. It shall be equipped with a "top-reading, spy-proof type dial." The UL label is considered adequate evidence of compliance with these requirements. Axial play on the level handle spindle shall not exceed 1/16 inch. The locks, lock bolt, door bolt operating cam, and bolt operating linkage connected thereto shall be protected by a tempered steel alloy hardplate located in front of the parts to be protected. Such hardplate to be at least 1/4 inch in thickness and to be in the Rockwell hardness range of C-63 to C-65. The front plate, edge plates, back plates, and cap sheet shall be of manufacturers' standard construction. The cap sheet of the door will have an inspection plate of such size that its removal will permit examination and inspection of the combination lock and operating cam area without removal of entire back cap sheet of the door.

5. Miscellaneous Opening. Omission of all miscellaneous openings is desirable, but not mandatory. However, in all instances openings for heating and ventilating ducts, pipes, and conduits shall not exceed 96 square inches in size. Pipes and conduits entering the vault shall enter through walls

---

1/ Vault doors are listed in the FSS (FSC Group 71, Part III, Section E, FSC Class 7110). Vaults equipped with doors that do not meet these specifications may qualify as strongrooms, if the construction meets the minimum requirements outlined in paragraph F of this appendix.

that are not common to the vault and the structure housing the vault. Preferably such pipes and conduits should be installed when the vault is constructed. If this is not practical, they shall be carried through snug-fitting pipe sleeves cast in the concrete. After installation, the annular space between the sleeve and the pipe or conduit shall be caulked solid with lead, wood, waterproof (silicone) caulking, or similar material, which will give evidence of surreptitious removal. The construction standards for man-safe barriers outlined in paragraph F-5 shall be followed when securing openings.

C. Class B Vault.

1. Floor. The floor should be a monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches thick.

2. Walls. The walls should be not less than 8-inch-thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used, and shall be used in seismic areas. Walls are to extend to the underside of the roof or ceiling above.

3. Roof/Ceiling. The roof or ceiling must be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements.

4. Vault Door and Frame Unit. See paragraph B3.

5. Lock. See paragraph B4.

6. Miscellaneous Openings. See paragraph B5.

D. Class C Vault.

1. Floor. See paragraph C1.

2. Walls. Walls must be not less than 8-inch-thick hollow clay tile (vertical cell double shells) or concrete blocks (thick shells). Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used. Where hollow clay tiles are used and such masonry units are flush, or in contact with, facility exterior walls, they shall be filled with concrete and steel-reinforced bars. Walls are to extend to the underside of the roof or ceiling above.

3. Roof/Ceiling. See paragraph C3.

4. Vault Door and Frame Unit. See paragraph B3.

5. Lock. See paragraph B4.

6. Miscellaneous Openings. See paragraph B5.

E. Structural Design. In addition to the requirements given above, the wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. For the vaults described above, the concrete shall be poured in place, and will have a minimum 28-day compressive strength of 2,500 pounds per square inch.

F. Strongrooms. A strongroom, as referred to in paragraph 14a(3)(f), shall be considered to be an interior space of the cleared facility or complex (see paragraph 3t) enclosed by, or separated from, other facility spaces by four walls, a ceiling, and a floor, all of which are constructed of solid building materials. Under this criterion, rooms having a false ceiling, and walls constructed of fabrics, wire mesh, or similar materials, shall not qualify as a strongroom. For strongrooms not located within a complex, the floor, ceiling, or wall(s) that is an exterior part of the building and less than 18 feet from the ground or from an access point, or adjoining another firm's space, shall be constructed as outlined in paragraphs C1, C3, and D2, respectively. Advice regarding use of solid building materials in strongroom construction may be provided by the CSO. Specific construction standards are as follows.

1. Hardware. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars, 2-inch square mesh of No. 11 gage wire (hereinafter referred to as "wire mesh"), 18 gauge expanded metal, hinges, pins, and the like, shall be securely fastened to preclude surreptitious entry and ensure visual evidence of tampering. Hardware accessible from outside the area shall be peened, brazed, or spot-welded to preclude removal.

2. Walls and Ceilings. Construction shall be of plaster, gypsum board, metal, hardboard, wood, plywood, or other solid, opaque materials offering similar resistance to, and evidence of, unauthorized entry into the area. Insert-type panels shall not be used. *

3. Floors. Floors shall be of solid construction, utilizing materials such as concrete, ceramic tile, and wood.

4. Windows. Window openings less than 18 feet from an access point (such as, another window outside the area, roof, ledge, or door) shall be fitted with 1/2 inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18 gauge expanded metal, or wire mesh securely fastened on the inside to preclude surreptitious removal. In addition to being kept closed at all times, the window shall be translucent or opaqued by any practical method, such as painting or covering the inside of the window.

5. Miscellaneous Openings. Openings for ducts, pipes, registers, sewers and tunnels of such size and shape as to permit unauthorized entry; for example, in excess of 96 square inches, shall be equipped with man-safe barriers such as wire mesh, 18 gauge expanded metal, or steel bars of at least 1/2 inch in diameter extending across their width with a maximum space of 6 inches between the bars. The steel bars shall be securely fastened at both ends to preclude removal, with crossbars to prevent spreading. Where wire

mesh, expanded metal, or steel bars are used, care shall be exercised to ensure that classified material within the room cannot be removed with the aid of any type of instrument.

6. Doors. Doors shall be substantially constructed of wood or metal. When windows, panels, or similar openings are used they shall be secured with 18 gauge expanded metal or wire mesh securely fastened on the inside. The windows shall be translucent or opaqued. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

7. Door Louvers and Baffle Plates. When used, they shall be reinforced with wire mesh fastened inside the room.

8. Door Locking Devices. Entrance doors shall be secured by either a built-in three-position dial-type changeable combination lock or a three-position dial-type changeable combination padlock, as specified in paragraph 14a(3)(d), which is secured to the door by a solid metal hasp.
Other (non-entry) doors shall be secured from the inside by a panic bolt *
(for example, activated by a panic bar); a dead bolt; a rigid wood or metal *
bar, which shall preclude "springing," that extends across the width of the *
door and is held in position by solid clamps, preferably on the door casing; *
or by any other means approved by the CSO. *

G. Approvals. The CSO and the contractor shall agree on the need to establish, and the extent of, the vault or strongroom prior to the award of the contract, when possible, or subsequently when the need for such areas becomes apparent during the performance on the contract.

Appendix V. REQUIREMENTS FOR THE CONSTRUCTION OF CLOSED AREAS

A. Application. This appendix specifies the minimum safeguards and standards required for the construction of closed areas that are used for safeguarding classified material, in accordance with the provisions of section IV of this manual. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used for evaluating the adequacy of existing areas.

B. Requirements.

1. Hardware. Heavy duty builder's hardware shall be used in construction, and all screws, nuts, bolts, hasps, clamps, bars, 2-inch square mesh of No. 11 gage wire (hereinafter referred to as "wire mesh"), 18 gauge expanded metal, hinges, pins, and so on, shall be securely fastened to preclude surreptitious removal and ensure visual evidence of tampering. Hardware accessible from outside the area shall be peened, pinned, brazed, or spot-welded to preclude removal.

2. Walls. Construction shall be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other opaque materials offering similar resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. Area barriers up to a height of 8 feet shall be of opaque or translucent construction, where visual access is a factor. If visual access is not a factor, the area barrier walls may be of wire mesh, or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area.

3. Windows. Window openings less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door,) shall be fitted with 1/2-inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18 gauge expanded metal, or wire mesh securely fastened on the inside. When visual access is a factor, the windows shall be kept closed and locked at all times, and shall also be made translucent or opaque by any practical method, such as painting or covering the inside of the glass. During non-duty hours, the windows shall be closed and securely fastened to preclude surreptitious removal of classified material.

4. Doors. Doors shall be substantially constructed of wood or metal. When windows, panels, or similar openings are used, they shall be secured with 18 gauge expanded metal or with wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be translucent or opaqued. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

5. Door Louvers or Baffle Plates. When used, they shall be reinforced with 18 gauge expanded metal or with wire mesh fastened inside the area.

6. Door Locking Devices. Entrance doors shall be secured with either a built-in three-position dial-type changeable combination lock, a three-position dial-type changeable combination padlock, as specified in paragraph 14a(3)(d), or with one of the key-operated padlocks with high security cylinders as described in paragraph 34a(3)(b)(2). Other doors shall be secured from the inside with a panic bolt (for example, actuated by a panic bar); a dead bolt; a rigid wood or metal bar (which shall preclude "springing"), which extends across the width of the door and is held in position by solid clamps, preferably on the door casing; or by other means approved by the CSO.

7. Ceilings. Ceilings shall be constructed of plaster, gypsum wallboard material, panels, hardboard, wood, plywood, ceiling tile, or other material offering similar resistance to and detection of unauthorized entry. Wire mesh, or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area may be used if visual access to classified material is not a factor. When wall barriers do not extend to the ceiling and a false ceiling is used it shall be reinforced with wire mesh, 18 gauge expanded metal, alarmed as outlined in paragraph 35, or otherwise secured with heavy-duty builder's hardware. (This feature also applies when panels are removable and entry can be gained into the area without visible detection.) When wire mesh or expanded metal are used, they must overlap the adjoining walls and be secured in a manner which precludes removal without leaving evidence of tampering. In those instances where barrier walls of an area extend to a solid ceiling, there is no necessity for reinforcing a false ceiling.

8. Ceilings (Unusual Cases). It is recognized that instances arise so that contractors may have a valid justification for not erecting a solid suspended ceiling as part of the areas, especially in high-ceilinged hangars. The contractor may state that it is impractical to use a suspended ceiling because of his or her production methods, such as the use of overhead cranes for the movement of bulky equipment within the area. There are also cases wherein the air conditioning system may be impeded by the construction of a solid suspended ceiling (for example, AIS Centers). At times, even the height of the classified material may make a suspended ceiling impractical. In such cases, special provisions shall be made to ensure that surreptitious entry to the area cannot be obtained by entering the area over the top of the barrier walls (such as, approved motion detection devices). Areas of this type should be closely scrutinized to ensure that the structural safeguards are adequate to preclude entry via adjacent pipes, catwalks, ladders, and the like, or observation, if visual access in a factor.

9. Miscellaneous Openings. Where ducts, pipes, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry, for example, in excess of 96 square inches, they shall be secured by 18 gauge expanded metal or wire mesh, or, where more practical, by steel bars at least 1/2-inch in diameter extending across their width, with a maximum space of 6 inches between the bars. The steel bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading. When wire mesh, expanded metal, or steel bars are used, care must be exercised to ensure that classified material cannot be removed through the openings with the aid of any type instrument. Care shall be taken to ensure that a barrier placed across any waterway (sewer or tunnel) will not cause clogging or offer obstruction to the free flow of water sewage.

Appendix VI. EXTRACTS OF THE ESPIONAGE AND SABOTAGE ACTS, OTHER FEDERAL CRIMINAL STATUTES, EXECUTIVE ORDER 12356, AND 32 CFR PART 2003 *

U.S.C. 18 § 371. Conspiracy to commit offense or to defraud the United States

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined not more than $10,000 or imprisoned not more than five years, or both.

U.S.C. 18 § 641. Public money, property or records

Whoever embezzles, steals, purloins or knowingly converts to this use or the use of another, or without authority, sells conveys or disposes of any records, voucher, money or thing of value of the United States or any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof or;

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted --

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

U.S.C. 18 § 793. Gathering, transmitting, or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States or any department or agency thereof, or with any person on behalf of the United

States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted, the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever, having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer --

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

U.S.C. 18 § 794. Gathering or delivering defense information to aid foreign governments

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war material of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification of defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

U.S.C. 18 § 795. Photographing and sketching defense installations

(a) Whenever, in the interests of national defense, the President defines certain vital military or naval installations or equipments as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined not more than $1,000 or imprisoned not more than one year, or both.

U.S.C. 18 § 796. Use of aircraft for photographing defense installations

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

U.S.C. 18 § 797. Publication and sale of photographs of defense installations

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

U.S.C. 18 § 798. Disclosure of classified information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information --

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes --

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section --

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

U.S.C. 18 § 799. Violation of regulations of the National Aeronautics and Space Administration

Whoever willfully shall violate, attempt to violate, or conspire to violate any regulation or order promulgated by the Administrator of the National Aeronautics and Space Administration for the protection of security of any laboratory, station, base or other facility, or part thereof, or any aircraft, missile, spacecraft, or similar vehicle, or part thereof, or other property or equipment in the custody of the Administration, or any real or personal property or equipment in the custody of any contractor under any contract with the Administration or any subcontractor of any such contractor, shall be fined not more than $5,000, or imprisoned not more than one year, or both.

U.S.C. 18 § 2153. Destruction of war material, war premises, or war utilities

(a) Whoever, when the United States is at war, or in times of national emergency as declared by the President or by the Congress, with intent to injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, or, with reason to believe that his act may injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, willfully injures, destroys, contaminates or infects or attempts to so injure, destroy, contaminate or infect so any war material, war premises, or war utilities, shall be fined not more than $10,000 or imprisoned not more than thirty years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy, shall be punished as provided in subsection (a) of this section.

U.S.C. 18 § 2154. Production of defective war material, war premises, or war utilities

(a) Whoever, when the United States is at war, or in times of national emergency as declared by the President or by the Congress, with intent to injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, or, with reason to believe that his act may injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities, willfully makes, constructs, or causes to be made or constructed in a defective manner, or attempts to make, construct, or cause to be made or constructed in a defective manner any war material, war premises or war utilities, or any tool, implement, machine, utensil, or receptacle used or employed in making, producing, manufacturing, or repairing any such war material, war premises or war utilities, shall be fined not more than $10,000 or imprisoned not more than thirty years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

U.S.C. 18 § 2155. Destruction of national-defense materials, national-defense premises or national-defense utilities

(a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully injures, destroys, contaminates or infects, or attempts to so injure, destroy, contaminate or infect any national-defense material, national-defense premises, or national-defense utilities, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

U.S.C. 18 § 2156. Production of defective national-defense material, national-defense premises or national-defense utilities

(a) Whoever, with intent to injure, interfere with, or obstruct the national defense of the United States, willfully makes, constructs, or attempts to make or construct in a defective manner, any national-defense material, national-defense premises or national-defense utilities, or any tool, implement, machine, utensil, or receptacle used or employed in making, producing, manufacturing, or repairing any such national-defense material, national-defense premises or national-defense utilities, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in subsection (a) of this section.

U.S.C. 50 § 421. Protection of indentities of certain United States Undercover Intelligence Officers, Agents, Informants, and Sources

(a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $50,000 or imprisoned not more than ten years, or both.

(b) Whoever, as a result of having authorized access to classified information, learns the identity of a covert agency and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $25,000 or imprisoned not more than five years, or both.

(c) Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined not more than $15,000 or imprisoned not more than three years, or both.

As used in this Section --

(1) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term "authorized," when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means --

(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency --

(i) whose identity as such an officer, employee, or a member is classified information, and

(ii) who is serving outside the United States or has within the last five years served outside the United States; or

(B) a United States citizen whose intelligence relationship to the United States is classified information, and --

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term "intelligence agency" means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term "United States," when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term "pattern of activities" requires a series of acts with a common purpose or objective.

U.S.C. 50 § 797. Security regulations and orders; penalty for violation

(a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, waterfront facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

PRESIDENTIAL DOCUMENTS

Title 3--
The President

Executive Order 12356 of April 2, 1982

National Security Information

TABLE OF CONTENTS

[FR Page]

Preamble....................[ ]

Part 1. ORIGINAL CLASSIFICATION

1.1 Classification Levels....................[ ]
1.2 Classification Authority....................[ ]
1.3 Classification Categories....................[ ]
1.4 Duration of Classification....................[ ]
1.5 Identification and Markings....................[ ]
1.6 Limitations on Classification....................[ ]

Part 2. DERIVATIVE CLASSIFICATION

2.1 Use of Derivative Classification....................[ ]
2.2 Classification Guides....................[ ]

Part 3. DECLASSIFICATION AND DOWNGRADING

3.1 Declassification Authority....................[ ]
3.2 Transferred Information....................[ ]
3.3 Systematic Review for Declassification....................[ ]
3.4 Mandatory Review for Declassification....................[ ]

Part 4. SAFEGUARDING

4.1 General Restrictions on Access....................[ ]
4.2 Special Access Programs....................[ ]
4.3 Access by Historical Researchers and Former Presidential Appointees.[ ]

Part 5. IMPLEMENTATION AND REVIEW

5.1 Policy Direction....................[ ]
5.2 Information Security Oversight Office....................[ ]
5.3 General Responsibilities....................[ ]
5.4 Sanctions....................[ ]

Part 6. GENERAL PROVISIONS

6.1 Definitions....................[ ]
6.2 General....................[ ]

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

ORIGINAL CLASSIFICATION

SECTION 1.1 CLASSIFICATION LEVELS

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

SEC. 1.2 CLASSIFICATION AUTHORITY.

(a) Top Secret. The authority to classify information originally as Top Secret may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; and

(3) officials delegated this authority pursuant to Section 1.2(d).

(b) Secret. The authority to classify information originally as Secret may be exercised only by:

(1) agency heads and officials designated by the President in the Federal Register;

(2) officials with original Top Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(c) Confidential. The authority to classify information originally as Confidential may be exercised only by:

(1) agency heads and officials designated by the President in the Federal Register;

(2) officials with original Top Secret or Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(d) Delegation of Original Classification Authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a), provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a), provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a), provided that official has been delegated original classification authority by the agency head.

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

SEC. 1.3 CLASSIFICATION CATEGORIES.

(a) Information shall be considered for classification if it concerns:

(1) military plans, weapons, or operations;

(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) foreign government information;

(4) intelligence activities (including special activities), or intelligence sources or methods;

(5) foreign relations or foreign activities of the United States;

(6) scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safeguarding nuclear materials or facilities;

(8) cryptology;

(9) a confidential source; or

(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably would be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

SEC. 1.4 DURATION OF CLASSIFICATION.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

SEC. 1.5 IDENTIFICATION AND MARKINGS.

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) one of the three classification levels defined in Section 1.1;

(2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(3) the agency and office of origin; and

(4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

SEC. 1.6 LIMITATIONS ON CLASSIFICATION.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.

Part 2

DERIVATIVE CLASSIFICATION

SEC. 2.1 USE OF DERIVATIVE CLASSIFICATION.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

SECTION 2.2. CLASSIFICATION GUIDES.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a); and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agency heads may, for good cause, grant and revoke waivers of the requirements to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

DECLASSIFICATION AND DOWNGRADING

SEC. 3.1 DECLASSIFICATION AUTHORITY

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a).

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

SEC. 3.2 TRANSFERRED INFORMATION.

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 Systematic Review for Declassification.

(a) The Archivist of the United States shall, in accordance with procedures and time frames prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

SEC. 3.4. MANDATORY REVIEW FOR DECLASSIFICATION

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

(1) the request is made by United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order.

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

SAFEGUARDING

SEC. 4.1 GENERAL RESTRICTIONS ON ACCESS.

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

SEC. 4.2 SPECIAL ACCESS PROGRAMS.

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

SEC. 4.3. ACCESS BY HISTORICAL RESEARCHERS AND FORMER PRESIDENTIAL APPOINTEES.

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

(1) are engaged in historical research projects, or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order, and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

IMPLEMENTATION AND REVIEW

SEC. 5.1 POLICY DIRECTION

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

SEC. 5.2 INFORMATION SECURITY OVERSIGHT OFFICE.

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies.

(2) oversee agency actions to ensure compliance with this Order and implementing directives;

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities, If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

SEC. 5.3 GENERAL RESPONSIBILITIES.

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the Federal Register to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

SEC. 5.4 SANCTIONS.

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official designated under Section 5.3(a) so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) Each agency head or the senior official designated under Section 5.3(a) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b)(1) or (2) occurs.

Part 6

GENERAL PROVISIONS

SEC. 6.1 DEFINITIONS

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

SEC. 6.2 GENERAL.

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Agency of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.

RULES AND REGULATIONS
INFORMATION SECURITY OVERSIGHT OFFICE
53F.R.38278-01, 32 CFR Part 2003
National Security Information; Standard Forms
Thursday, September 29, 1988

Agency: Information Security Oversight Office (ISOO).

Action: Final rule.

Summary: This amendment to 32 CFR 2003.20 provides for: (1) the issuance and use of STANDARD FORM 312, "Classified Information Nondisclosure Agreement" (SF 312); and (2) the modification of Paragraph 1 of all previously executed copies of STANDARD FORM 189, "Classified Information Nondisclosure Agreement" (SF 189), to strike the word "classifiable" and to substitute in its place language that clarifies the scope of "classified information" as used in those agreements. From the effective date of this rule, the SF 312 shall be used in lieu of its predecessor nondisclosure agreements, SF 189 and STANDARD FORM 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)" (SF 189-A). ISOO is issuing the SF 312 as a preferred means of clarifying the scope of some language in the SF 189 and the SF 189-A that has been at issue in litigation concerning the constitutionality and legality of certain nondisclosure agreements, including the SF 189. Notwithstanding the changes in some of its language, the SF 312 does not in any way differ from its predecessor nondisclosure agreements with respect to the substance of the information that each is intended to protect. ISOO is clarifying executed copies of the SF 189 to comply with a recent order of the United States District Court for the District of Columbia, to take account of statutory provisions that reflect congressional concern regarding possible ambiguity of the word "classifiable," and to make the language of the SF 189 more consistent with the language of the SF 312 and the SF 189-A.

Effective Date: September 29, 1988.

For further information contact: Steven Garfinkel, Director, ISOO, (202) 535-7251.

Supplementary Information: This amendment to 32 CFR Part 2003 is issued pursuant to section 5.2(b)(7) of Executive Order 12356, "National Security Information," which grants the Director of ISOO the authority to issue standardized security forms, and Paragraph 1 of National Security Decision Directive 84, March 11, 1983, which directs ISOO to issue a standardized nondisclosure agreement to be signed as a condition of access by all persons cleared for access to classified information. In fulfilling this requirement, ISOO has previously issued two nondisclosure agreements: SF 189, "Classified Information Nondisclosure Agreement," in September 1983; and SF 189-A, "Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government)," in November 1986.

On December 29, 1987, ISOO directed agencies to halt further implementation of the SF 189 and SF 189-A as a result of the enactment of section 630 of the Treasury, Postal Service, and General Appropriations Act, 1988, which was part of the Omnibus Continuing Resolution for Fiscal Year 1988 (Public Law 100-202). On May 27, 1988, in litigation primarily involving the constitutionality and legality of the SF 189, the United States District Court for the District of Columbia ruled that Section 630 of Public Law 100-202, is unconstitutional (National Federation of Federal Employees v. United States, et al, Civil Action No. 87-2284-OG; American Federation of Government Employees, et al v. Garfinkel, et al, Civil Action No. 87-2412.OG; American Foreign Service Association, et al v. Garfinkel, et al, Civil Action No. 88-0440-OG). In a subsequent ruling of July 28, 1988, in the first two of the above-captioned cases, the same court upheld the constitutionality and legality of the SF 189. However, the court also ruled that in order to bring the scope of the word "classifiable" within constitutional limits, the SF 189 must be modified, either (a) by providing each signatory a copy of ISOO's definition of "classifiable information," as published in 52 FR 48367 on December 21, 1987; or (b) by striking the word from executed copies of the agreement. Notwithstanding these rulings upholding the validity of the predecessor nondisclosure agreements, ISOO has concluded that, in lifting the moratorium on the execution of required nondisclosure agreements, a preferred means to deal with the perceived ambiguities in their language is the issuance of a new nondisclosure agreement, the SF 312. The SF 312 avoids as many of these perceived problem areas as possible without changing the substance of the classified information that the nondisclosure agreement is intended to protect. In issuing the SF 312, ISOO does not seek its execution by every cleared Government or industry employee who has already executed an SF 189 or an SF 189-A, since these total over two million individuals. However, the rule provides that every individual who previously signed an SF 189 or SF 189-A may substitute a signed copy of the SF 312 at his or her own choosing. Also, through this rule ISOO is instructing agencies to enforce the predecessor agreements in a manner that is fully consistent with the enforcement of the SF 312. To help achieve greater consistency, ISOO is complying with the court order by opting to strike the word "classifiable" from the SF 189, while substituting language that clarifies the scope of "classified information," as used in the agreement. This language is taken from the definition of "classifiable" previously published in the Code of Federal Regulations, and adjudged by the District Court to bring the definition within constitutional and legal standards. ISOO has not included the word "classifiable" in the SF 312, and did not previously include it in the SF 189-A, although these agreements are both intended to protect the same information protected by the SF 189. The word "classifiable" had been included in the SF 189 not to introduce concepts separate and distinct from classified information, but to emphasize the need to protect unmarked classified information and information in the process of a classification determination. Therefore, striking the word from the SF 189 is the more consistent of the two options presented by the court, while its concepts remain protected within the scope of classified information.

Concurrent with the issuance of the SF 312, by a letter of this date the ISOO Director is instructing the senior official for information security oversight in each agency that creates or handles classified information to lift the current moratorium on the execution of the "Classified Information Nondisclosure Agreement," imposed by letter of December 29, 1987; and to lift the moratorium on the withdrawal of access to classified information and security clearances, imposed by letter of August 21, 1987, for those cleared persons who refuse to sign the SF 312.

Before issuing the SF 312, ISOO submitted drafts for review and comment to the executive branch agencies most affected by it; to seven Committees or Subcommittees of the Congress most involved with the subject of classified information; and to selected interest groups actively concerned with this subject. ISOO has considered those comments that it has received in response to its solicitations, and, when ISOO concluded that suggested changes were warranted, it has incorporated these into the SF 312 or this implementing rule. As required by National Security Decision Directive 84, the Department of Justice has concluded that the SF 312 is enforceable in a civil action brought by the United States.

This is not a major rule for purposes of Executive Order 12291.

List of Subjects in 32 CFR Part 2003

Classified Information, Executive Orders, Information, National Security Information, Security Information.

32 CFR Part 2003 is amended as follows:

PART 2003--NATIONAL SECURITY INFORMATION--STANDARD FORMS

1. The authority citation for 32 CFR Part 2003 continues to read:

Authority: Section 5.2(b)(7) of E.O. 12356.

Subpart B--Prescribed Forms

2. Section 2003.20 is revised to read as follows:

§ 2003.20 Classified Information Nondisclosure Agreement: SF 312; Classified Information Nondisclosure Agreement: SF 189; Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government): SF 189-A.

(a) SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual. The prior execution of at least one of these agreements, as appropriate, by an individual is necessary before the United States Government may grant that individual access to classified information. From the effective date of this rule, September 29, 1988, the SF 312 shall be used in lieu of both the SF 189 and the SF 189-A for this purpose. In any instances in which the language in the SF 312 differs from the language in either the SF 189 or SF 189-A, agency heads shall interpret and enforce the SF 189 or SF 189-A in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

(b) All employees of executive branch departments, and independent agencies or offices, who have not previously signed the SF 189, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(c) All Government contractor, licensee, and grantee employees, or other non-Government personnel requiring access to classified information in the performance of their duties, who have not previously signed either the SF 189 or the SF 189-A, must sign the SF 312 before being granted access to classified information. An employee who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies, with the cooperation of the pertinent contractor, licensee or grantee, shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(d) Agencies may require other persons, who are not included under paragraphs (b) or (c) of this section, and who have not previously signed either the SF 189 or the SF 189-A, to execute SF 312 before receiving access to classified information. A person in such circumstances who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(e) The use of the "Security Debriefing Acknowledgement" portion of the SF 312 is optional at the discretion of the implementing agency.

(f) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee or grantee of another United States agency, provided that an authorized United States Government official or, for non-Government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.

(g) The provisions of the SF 312, the SF 189, and the SF 189-A do not supersede the provisions of section 2302, Title 5, United States Code, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(h) Modification of the SF 189. The second sentence of Paragraph 1 of every executed copy of the SF 189 is clarified to read:

(1) As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive Order or statute that prohibits the unauthorized disclosure of

information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive Order or statute that requires protection for such information in the interest of national security.

(2) Scope of "classified information." As used in the SF 312, the SF 189, and the SF 189-A, "classified information" is marked or unmarked classified information, including oral communications; and unclassified information that meets the standards for classification and is in the process of a classification determination, as provided in sections 1.1(c) and 1.2(e) of Executive Order 12356 or any other statute or Executive Order that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination.

(3) Basis for liability. A party to the SF 312, SF 189 or SF 189-A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that: (i) the marked or unmarked information is classified, or meets the standards for classification and is in the process of a classification determination; and (ii) his or her action will result, or reasonably could result in the unauthorized disclosure of that information. In no instance may a party to the SF 312, SF 189 or SF 189-A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

(i) Points of clarification.

(1) As used in Paragraph 3 of the SF 189 and SF 189-A, the word "indirect" refers to any situation in which the knowing, willful or negligent action of a party to the agreement results in the unauthorized disclosure of classified information even though the party to the agreement does not directly communicate, deliver or transmit classified information to a person who is not authorized to receive it.

(2) As used in Paragraph 7 of the SF 189, "information" refers to "classified information," exclusively.

(3) As used in the third sentence of Paragraph 7 of SF 189 and SF 189-A, the words "all materials which have, or may have, come into my possession," refer to "all classified materials which have or may come into my possession," exclusively.

(j) Each agency must retain its executed copies of the SF 312, SF 189, and SF 189-A in file systems from which the agreements can be expeditiously retrieved in the event that the United States must seek their enforcement. The copies or legally enforceable facsimiles of them must be retained for 50 years following their date of execution. An agency may permit its contractors, licensees and grantees to retain the executed agreements of their employees during the time of employment. Upon the termination of employment, the contractor, licensee or grantee shall deliver the SF 312, SF 189, or SF 189-A of that employee to the Government agency primarily responsible for his or her classified work.

(k) Only the National Security Council may grant an agency's request for a waiver from the use of the SF 312. To apply for a waiver, an agency must submit its proposed alternative nondisclosure agreement to the Director of ISOO, along with a justification for its use. The Director of ISOO will request a determination about the alternative agreement's enforceability from the Department of Justice prior to making a recommendation to the National Security Council. An agency that has previously received a waiver from the use of the SF 189 or the SF 189-A need not seek a waiver from the use of the SF 312.

(l) The national stock number for the SF 312 is 7540-01-280-5499, dated: September 23, 1988.

Steven Garfinkel
Director, Information Security Oversight Office.
[FR Doc. 88-22232 Filed 9-26-88; 8:45 am]

Appendix VII. GUIDANCE FOR PREPARATION OF SECURITY BRIEFINGS

A. Defensive Security Briefings.

1. General. A defensive security briefing containing elements of the following outline shall be given to those individuals or employees so identified in paragraph 5u.

2. Introduction. National policy over the past several years has encouraged the expansion of cultural, trade, and commercial ties with Designated countries. As a result, an increasing number of representatives from Designated countries are coming to the U.S. on trade visits, cultural visits, East-West exchange visits, and the like. Similarly, representatives of U.S. industry have been, with increasing regularity, making reciprocal visits to Designated countries. These expanding marketing opportunities carry with them a parallel responsibility for ensuring that certain categories of information are not released, and, where appropriate, proper authorization is obtained prior to release.

a. U.S. citizens who have had access to classified defense information are important targets for hostile intelligence services. It is common practice for hostile intelligence services to establish and maintain dossiers on personnel of intelligence interest, particularly of personnel whose jobs afford them access to vital defense information in any area of special interest. These services are constantly on the alert for opportunities to gain any kind of advantage that can be exploited, regardless of the country visited.

b. The intelligence network of the Designated counties is worldwide and ever present. These intelligence agencies have concentrated on those fields which involve scientific and military knowledge possessed by the Western powers. A key source of technical and scientific information are the numerous conventions, seminars, conferences, and symposia held throughout the world each year. Other means of obtaining information is through the tight, police-like controls over the movements of all personnel visiting Designated countries. Travelers may be "targeted" the moment they apply for a visa. Under such controlled conditions, there is little that can be done to prevent espionage efforts and harassments directed against selected individuals.

c. It must be remembered that Designated country intelligence and security services carry espionage activities to fantastic lengths. While the techniques that are employed may seem far-fetched or illicit, they are in fact used in day-to-day activities and operations. Travelers must recognize them as a part of the Designated system, so that they may successfully counter such practices. A publication entitled, "A Study of Harassments and Provocations," illustrates procedures used by Designated country intelligence and security services, and is intended to support official defensive security briefings for persons with authorized access to classified information who are traveling to such countries. Copies of this publication may be requested from the CSO.

3. Export Controls. The U.S. Government, by statute, E.O., and administrative policy, has established a number of procedures designed to control the export of certain categories of information. One of its primary objectives is the control of the export of scientific and technical information to ensure that information made available to Designated countries does not work to the detriment of the U.S. national interest. Among the existing controls are:

a. a system for classifying national security information and strictly controlling its dissemination (E.O. 12356);

b. a system to control the export of arms, ammunition, and implements of war, including unclassified technical data and information relating thereto (see the ITAR issued by the Department of State); and

c. a system to control the export of U.S. commodities and unclassified technical data which would make a significant contribution to the military potential of any other nation or nations which would prove detrimental to the national security of the U.S. (see the Export Administration Regulations issued by the Department of Commerce).

4. Marketing Activities With Designated Countries. It must be recognized that marketing personnel are in a particularly difficult role. On the one hand they must be in a position to knowledgeably discuss their products and employ all of the attributes of good salesmanship to promote a free exchange of information in order to successfully conclude marketing endeavors. On the other hand, a clear understanding of, and strict adherence to, the controlling regulations are necessary for those categories of information which cannot be disclosed, or which require prior U.S. Government approval in order to be disclosed. Marketing personnel, who meet with representatives from Designated countries, should be thoroughly versed and totally knowledgeable with respect to what information may be released. Meticulous preplanning is essential if U.S. security interests and responsibilities are to be properly met. The following categories of information merit special consideration before planning a meeting with representatives from Designated countries.

a. Disclosure of Classified Information. Obviously, classified information may not under any circumstances be disclosed to representatives from Designated countries. It cannot be assumed that all personnel are thoroughly familiar with respect to what is and what is not classified. A thorough reassessment and evaluation of pertinent information should be undertaken to ensure a complete and unequivocal understanding as to what is and what is not classified.

b. Unclassified Information Relating to Classified Contracts. Before a contractor may disclose any information that pertains to a classified contract or project, the contractor must obtain the approval of DoD as provided for in section I, paragraph 5o. It is essential to ensure that all personnel who will participate in visits by representatives of Designated countries are thoroughly knowledgeable with respect to that information which relates to classified contracts, and which therefore may not be released without prior approval of DoD.

c. Information That Comes Within the Purview of the International Traffic in Arms Regulations. The ITAR applies not only to the export of arms, ammunition, and implements of war, but also to both classified and unclassified technical data related thereto. Disclosure to a representative of a Designated country within the U.S. or abroad constitutes an export under the provisions of these regulations. Further information concerning these requirements may be obtained from the Office of Munitions Control, Department of State, Washington, D.C. 20520.

d. Technical Data Subject to Export Control. Unclassified technical data, pertaining to items on the "Commodity Control List" may require approval by the Department of Commerce prior to release to a representative of a Designated country. Part 379, Technical Data, Export Administration Regulations, issued by the Department of Commerce pursuant to the Export Administration Act of 1969, as amended, sets forth the rules applicable to the export of technical data. Release of such information to a representative of a Designated country within this country or abroad constitutes an export under these regulations. For further information in this connection, inquiries should be addressed to the local U.S. Department of Commerce District Office, or to the Office of Export Administration, Department of Commerce, Washington, D.C. 20230.

5. Conclusion. Attention to this very difficult and complex area is essential if U.S. national interests are to be properly safeguarded, and if the contractor is to abide by the DD Form 441 with DoD and with the applicable U.S. statutes, as enumerated above. In the case of any information which may be classified or any information relating to a classified contract, the contractor should initiate appropriate consultation with his or her contracting officer. Whenever there is any doubt or question with respect to other information, consultation may be necessary with the Office of Munitions Control, Department of State and/or the Office of Export Administration, Department of Commerce. If there is any doubt, or if there are further questions, ask the CSO. In all situations, be sure that information disclosed to representatives of Designated countries is appropriate for release to these countries. If in doubt, do not provide the information. Although the emphasis in this guide has been placed on the procedures to be followed when engaged in marketing activities with representatives of Designated countries, generally, these same procedures are applicable when dealing with representatives of any other foreign countries.

B. Counterintelligence Awareness Briefings.

1. General. A counterintelligence awareness briefing containing elements of the following material, or updated information, shall be given to appropriate individuals or employees.

2. Introduction. The following elements of information are intended to be neither all-inclusive nor all-exclusive, but should be used as source material in the preparation of counterintelligence awareness briefings and as a guide for the type of information to be included in this type of briefing. Routine, stereotyped briefings not only fail to meet intended objectives, but could actually weaken security by giving the recipient a false sense of security. Only the use of thoughtfully prepared briefings, based on authoritative information and related to the duties performed, and the sensitivity of the

classified information to which exposed and manner of presentation, will accomplish the purpose. The following information has been extracted, with permission, from a pamphlet published by the Federal Bureau of Investigation, "Secrets, Spies and Citizens." Copies of the pamphlet may be requested from the local FBI office. Additional current topical material may be requested from these offices or from local military intelligence activities.

3. The Threat. Intelligence collection -- the world of espionage and counterespionage, spies, and spy catchers -- is a popular subject of fiction. It has been the topic of countless books, short stories, TV serials, and movies. The role of the spy, the "Secret Agent," has become so sensationalized and exaggerated that it is very easy to think that spies exist only in the minds of fiction writers -- that spying belongs in the same category as science fiction and westerns. Do not believe it. Spies do exist, and literally thousands of spies, or intelligence officers, as they are officially known, and their agents are at this moment plying their treacherous trade within the U.S. The principal source of these intelligence officers is the Soviet Union, but the USSR's allied nations in Eastern Europe, as well as Cuba, the People's Republic of China, and smaller Asian Designated nations such as North Korea and Vietnam, also dispatch spies to U.S. shores.

a. The Objectives and Techniques of Spies. Their main objective is the wholesale collection of data. The most prized type of intelligence data is the classified government document, but unclassified material -- even material which appears to be trivial -- can also be of inestimable value. In their task of gathering intelligence data, the foreign intelligence services have a large array of tools. Satellites miles above the earth's surface gather photographic data. Aircraft and vessels gather electronic intelligence. But a further source of data, and potentially the most valuable to a hostile nation, is that acquired through the use of actual spies. (Here the briefer may wish to identify the type of classified projects or work being performed by the facility which lends credence to possibility of its being an espionage target.) Intelligence services may gather their information through the use of several different techniques. Probably the greatest achievement an intelligence organization can have is the placement or recruitment of an agent directly in a sensitive position in a national defense or intelligence element of an opposing government. The penetration by live or electronic sources of private institutions involved in sensitive, national defense-related research and development work can also be of tremendous value.

(1) Hostile intelligence collectors ply Washington and other locations where strategic data can be collected. They gain their desired information wherever, whenever, and from whomever it can be had. Hostile intelligence officers employ various tactics in their campaigns to enlist target employees. They may use a honeyed, seemingly guileless approach. They befriend targets, treat them to gifts and money, wine and dine them. Many Soviet and other Designated agents believe that Americans are hopeless materialists, and can be easily swayed by appeals to their alleged greed.

(2) In another maneuver, a hostile intelligence officer misrepresents him or herself as a citizen of a country friendly to the U.S. Thus a targeted American may be duped into handing over sensitive information by being led to believe that he or she is aiding an ally to

the U.S. In variation of this tactic, an intelligence officer poses as a representative of a non-Designated country towards which a targeted American is particularly sympathetic. Also, if a hostile agent believes that an individual has Designated or similar sympathies, he or she may make an appeal for information based on ideology. A "pitch" for information may also be geared to take advantage of an American's desire for international harmony and world peace.

(3) Another favored appeal exploits the American belief in freedom of speech and the free exchange of information. A hostile intelligence officer in the role of a scientist may, for example, tell an American scientist that science has no political boundaries. Therefore, in the interest of science, the American is encouraged to share his or her knowledge with a fellow "member" of the international scientific community. Intelligence agents can also play rough in their ceaseless quest for strategic information. To such people espionage is a business. If they feel coercion and blackmail will serve their purpose, they will not hesitate to employ those methods. The honeyed approach can readily turn sour if an agent determines that a targeted employee has personal inadequacies which that employee does not wish to have exposed.

(4) Correspondingly, another tactic is the exploitation of a "hostage situation." If, for example, a foreign intelligence service learns that a target employee has relatives in Eastern Europe or the USSR, that employee is in an extremely vulnerable position. First will come gentle persuasion (an agent may produce "letters" from so-called relatives calling for the American to "cooperate"). If that does not work, the agent may suggest that harsh measures could be applied to the relatives.

b. Recognizing the Approach.

(1) One should therefore be wary of glad-handing strangers who make an intensive effort at forming a friendship, and then slowly but surely begin to use that friendship to learn where one works, the nature of one's assignment, and who one works with. A generous and inquisitive stranger could very well be the proverbial wolf in sheep's clothing.

(2) One should also be wary of strangers who ask for information not related to their professed area of interest or do not seem to be particularly knowledgeable in their field. Thus, if "scientists" request data not related to their fields, or do not seem to know much about their supposed areas of expertise, then they could very well be impostors.

(3) The operative of a foreign intelligence service need not be a foreigner, nor need the occasion of encountering him or her be in any way extraordinary. The neighbor one might meet at a PTA meeting could be a foreign diplomat who lives down the block, or he or she could be a fellow American who has been recruited as an agent by a hostile service. The spy could be a "spotter," who reports to an intelligence service on persons he or she meets who appear to be susceptible to recruitment and, sometimes, arranges for intelligence officers to meet them. Do not expect either intelligence officers or agents to expose their roles in any dramatic and sudden fashion. Usually there is a long period of cultivation during which conversations with

the individual could be completely normal and innocuous. However, at any point where someone begins to inquire into aspects of one's knowledge or activity which are classified or otherwise private, one should certainly stop to consider whether the inquiry is normal innocent curiosity, or whether it might be the beginning of an attempt to secure intelligence information for the benefit of another country.

c. Protecting the Bits & Pieces. It cannot be overemphasized that unclassified material may be just as valuable to a foreign intelligence service as classified material. In formulating their estimations of U.S. strengths and weaknesses, and in the quest for data that will enhance their own nation's strength, foreign intelligence services seek all types of material. A small bit of information could represent a very important piece in a much larger puzzle. Therefore, all data should be protected from the probing hands of foreign agents. A stolen industrial process can save thousands of dollars in research and development cost. The most trivial document could be the missing link of a hostile nation's problem.

d. Reporting the Threat. In the effort to protect America's secrets, the role of the facility must be emphasized. Each U.S. Government agency and private industry which deals with classified material has a specified official in charge of security matters. This security officer should be recognized as an ally and not an adversary. If approached by a suspicious stranger in the manner described above, the security officer should be informed immediately of the encounter. Even if a friendship has been established, even if the individual has been able to pry loose some information, the security officer should be consulted. A major aspect of the security officer's job is to protect employees from getting involved in compromising situations and, if necessary, to extricate them from such situations. Such assistance cannot be rendered if the employee remains silent. Of course, it is much better for an employee to reveal a suspect relationship voluntarily, rather than have it come to light in the course of a security investigation, or through some other means. Then, it may be too late for anyone to assist the indiscreet employee. Basically, it cannot be overemphasized that, if involved in a compromising situation, the sooner the employee consults his or her facility security officer, the better. Of course, sometimes one will be in a place or situation where one cannot, or for some reason does not want to, contact the security officer. Remember that in the U.S., the FBI is as close as the nearest telephone. Directions for contacting FBI offices appear in the front of all U.S. telephone books. Abroad, the nearest U.S. diplomatic establishment can arrange to put one in touch with the FBI or other appropriate U.S. Government security officials. Once again, it must be stressed that the best course of action in any of the questionable situations mentioned herein is to immediately relate the facts to a counterintelligence professional who will be able to analyze the situation and propose a course of action. Effective counterintelligence is a demanding and professional discipline, and any attempts by untrained or uninformed amateurs to handle hostile efforts on their own could not only result in personal disaster, but also could interfere with the FBI's coordinated counterattack.

e. Summary of Threat. Finally, it must be stressed that the threat posed by foreign intelligence agencies cannot be underestimated. History is replete with situations in which a nation's security was greatly damaged by the efforts of a hostile nation's intelligence services. In

American history, the breaking of the Japanese secret code helped to bring U.S. victory in the Pacific during World War II. On the other hand, the theft of some key U.S. atomic secrets greatly abetted the interests of the Soviet Union. The craft of spies is by no means a game. The very fate of nations can be damaged or enhanced by their enterprises.

4. Summary -- Counterintelligence Awareness is Critical. The Soviet Union and its surrogates have established a long standing, well-organized, deliberate, and quite successful effort to acquire and utilize Western state-of-the-art technology by both overt and covert means. Unquestionably, this acquisition of Western technology has played, and will continue to play, an extremely important role in the development of industrial and military capabilities of Designated countries, particularly the Soviet Union. A philosopher once said, "Knowledge itself is power." This maxim most certainly applies to national power, for one gauge of national power is the amount and quality of scientific, technological, and military-related knowledge possessed by a nation. A nation such as the U.S. can be weakened by the theft of its vital knowledge, and its enemies can be strengthened by the acquisition of that knowledge, whether it be classified or unclassified. It is the responsibility of each individual who has been entrusted with sensitive data to do his or her share in protecting America's strategic knowledge, whether it be classified TOP SECRET or seemingly unimportant, unclassified material. For if Americans do not conduct themselves in a responsible and patriotic manner, do not recognize that this country's national security is based essentially on the loyalty and efforts of its citizens, then the tightest document classification system, the most efficient security organizations, and the mightiest Armed Forces may be utterly valueless.

Appendix VIII. INFORMATION REGARDING COGNIZANT SECURITY OFFICES, DISCO, DSI, AND OISI

OPERATIONAL AREAS OF DIS COGNIZANT SECURITY OFFICES

New England Region (S1110) -- formerly known as the Boston Region

The New England Region includes: the states of Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont; and the following counties in New York:

Albany
Allegany
Broome
Cattaraugus
Cayuga
Chautauqua
Chemung
Chenango
Clinton
Columbia
Cortland
Delaware
Dutchess
Erie
Essex
Franklin
Fulton
Genesee
Greene
Hamilton
Herkimer
Jefferson
Lewis
Livingston
Madison
Monroe
Montgomery
Niagara
Oneida
Onandaga *
Ontario
Orleans
Oswego
Otsego
Rensselaer
St. Lawrence
Saratoga
Schenectady
Schoharie
Schuyler *
Seneca
Steuben
Sullivan
Tioga
Tompkins
Ulster
Warren
Washington *
Wayne
Wyoming
Yates

Mid-Atlantic Region (S1410) -- formerly known as the Philadelphia Region

The Mid-Atlantic Region includes: the states of Delaware, New Jersey, Pennsylvania, West Virginia, Maryland (less the counties of Anne Arundel, Baltimore, Calvert, Charles, Harford, Howard, Montgomery, Prince Georges, and St. Marys); and the following counties in New York:

Bronx
Kings (Brooklyn)
Nassau
New York (Manhattan)
Orange
Putnam
Queens
Richmond
Rockland
Suffolk
Westchester

Capital Region (S1510) -- formerly known as the Washington Region

The Capital Region includes: the state of Virginia; Washington, D.C.; and the following counties in Maryland: Anne Arundel, Baltimore, Calvert, Charles, Harford, Howard, Montgomery, Prince Georges, and St. Marys.

Mid-Western Region (S3210) -- formerly known as the Cleveland Region

The Mid-Western Region includes: the states of Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin; and the following counties in Illinois:

Adams
Boone
Brown
Bureau
Carroll
Cass
Champaign
Christian
Clark
Coles
Cook
Crawford
Cumberland
De Kalb
De Witt
Douglas
Du Page
Edgar
Effingham
Ford
Fulton
Grundy
Hancock
Henderson
Henry
Iroquois
Jasper
Jo Daviess
Kane
Kankakee
Kendall
Knox
Lake
La Salle
Lee
Livingston
Logan
Macon
Marshall
Mason
McDonough
McHenry
McLean
Menard
Mercer
Morgan
Moultrie
Ogle
Peoria
Pike
Piatt
Putnam
Rock Island
Sangamon
Schuyler
Scott
Shelby
Stark
Stephenson
Tazewell
Vermilion
Waren
Whiteside
Will
Winnebago
Woodford

And the following counties in Missouri:

Adair
Andrew
Atchison
Bates
Benton
Boone
Buchanan
Caldwell
Callaway
Jackson
Johnson
Knox
Lafayette
Lewis
Linn
Livingston
Macon
Mercer

Carroll
Cass
Chariton
Clark
Clay
Clinton
Cole
Cooper
Daviess
De Kalb
Gentry
Grundy
Harrison
Henry
Holt
Howard
Moniteau
Nodaway
Pettis
Platte
Putnam
Randolph
Ray
Saline
Schuyler
Scotland
Shelby
Sullivan
Worth

Southeastern Region (S4110) -- formerly known as the Atlanta Region

The Southeastern Region includes: the states of Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, North Carolina, South Carolina, and Tennessee; Puerto Rico, and U.S possessions in the Atlantic and Caribbean areas.

Southwestern Region (S4210) -- formerly known as the St. Louis Region

The Southwestern Region includes: states of Arizona, Colorado, New Mexico, Oklahoma, Texas; and the following counties in Illinois:

Alexander
Bond
Calhoun
Clay
Clinton
Edwards
Fayette
Franklin
Gallatin
Greene
Hamilton
Hardin
Jackson
Jefferson
Jersey
Johnson
Lawrence
Macoupin
Madison
Marion
Massac
Monroe
Montgomery
Perry
Pope
Pulaski
Randolph
Richland
Saline
St. Clair
Union
Wabash
Washington
Wayne
White
Williamson

and the following counties in Missouri:

Audrain
Barry
Barton
Bollinger
Butler
Camden
Cape Girardeau
Carter
Cedar
Christian
Crawford
Dade
Dallas
Dent
Douglas
Dunklin
Franklin
Gasconade
Greene
Hickory
Howell
Iron
Jasper
Jefferson
Laclede
Lawrence
Lincoln
McDonald
Madison
Maries
Marion
Miller
Mississippi
Monroe
Montgomery
Morgan
New Madrid
Newton
Oregon
Osage
Ozark
Pemiscot
Perry
Phelps
Pike
Pulaski
Polk
Ralls
Reynolds
Ripley
St. Clair
St. Charles
St. Francois
Ste. Genevieve
St. Louis
Scott
Shannon
Stoddard
Stone
Taney
Texas
Vernon
Warren
Washington
Wayne
Webster
Wright

Northwestern Region (S5210) -- formerly known as the San Francisco Region

The Northwestern Region includes: the states of Alaska, Idaho, Montana, Oregon, Utah, Washington, and Wyoming; and the following counties in California:

Alameda
Alpine
Amador
Butte
Calaveras
Colusa
Napa *
Nevada *
Placer
Plumas
Sacramento
San Benito

Contra Costa
Del Norte
El Dorado
Fresno
Glenn
Humboldt
Inyo
Kings
Lake
Lassen
Madera
Marin
Mariposa
Mendocino
Merced
Modoc
Mono
Monterey
San Francisco
San Joaquin
San Mateo
Santa Clara
Santa Cruz
Shasta
Sierra *
Siskiyou
Solano
Sonoma
Stanislaus
Sutter
Tehama
Trinity
Tulare
Tuolumne
Yolo
Yuba

Carson City, Nevada, and the following counties in Nevada:

Churchill
Douglas
Elko
Eureka
Humboldt
Lander
Lyon
Mineral
Pershing
Storey
Washoe
White Pine

Pacific Region (S5310) -- formerly known as the Los Angeles Region

The Pacific Region includes: the state of Hawaii, U.S. possessions and trust territories in the Pacific area, and the following counties in California:

Imperial
Kern
Los Angeles
Orange
Riverside
San Bernardino *
San Diego
San Luis Obispo
Santa Barbara
Ventura

and the following counties in Nevada:

Clark
Esmeralda
Lincoln
Nye

TELEPHONE NUMBERS AND ADDRESSES

The following listing contains the addresses and telephone numbers of the PIC-CVA and the CSO's. The following indicated numbers and addresses shall be used to obtain the required verification of facility clearance and safeguarding capability of prospective contractors and subcontractors (see paragraphs 58 and 59). Correspondence should be addressed to the Defense Investigative Service, Director of Industrial Security (appropriate address as cited below).

	Address	Area Code	Telephone Number	AUTOVON NO.
PIC-CVA Central Verifications Activity	P.O. Box 1211 Baltimore, MD 21203-1211	301	633-4820	
Capital Region	2461 Eisenhower Avenue Alexandria, VA 22331-1000	202	325-9395	221-9395
Mid-Atlantic Region	1040 Kings Highway North Cherry Hill, NJ 08034-1908	609	482-6500 (ask for clearance verification)	
Mid-Western Region	610 S. Canal Street, Room 908 Chicago, IL 60607-4577	312	886-2437	
New England Region	Barnes Building 495 Summer Street Boston, MA 02210-2192	617	451-4927/3052	955-4927/3052
Northwestern Region	Presidio of San Francisco Bldg. 35, Room 114 San Francisco, CA 94129-7700	415	561-3251	586-3251
Pacific Region	3605 Long Beach Blvd., Suite 405 Long Beach, CA 90807-4013	213	595-7644/52	
Southeastern Region	2300 Lake Park Drive, Suite 250 Smyrna, GA 30080-7606	404 404 (after 4:00 p.m.)	432-0826 432-1822	697-6783
Southwestern Region	P.O. Box 88900 St. Louis, MO 63188-1900	314	263-5061	693-5061

The following are the telephone numbers for the DIS Directors of Industrial Security. These numbers may be used for all matters other than verifications of facility clearances and safeguarding capability. The mailing address is the same as that listed above.

CSO Region	Area Code	Telephone Number	AUTOVON NO. (For Gov't. Agencies Use)
Capital	202	325-9634/5	221-9634/5
Mid-Atlantic	609	482-6500	444-4030/1
Mid-Western	312	886-2436	-
New England	617	451-4914/6	955-4914/6
Northwestern	415	561-3235/6	586-3235/6
Pacific	213	595-7251	-
Southeastern	404	432-0826	697-6783
Southwestern	314	263-5498	693-5498

The following listing contains the addresses and telephone numbers of DISCO, DSI, and OISI.

City & State	Address	Area Code	Telephone Number	AUTOVON NO. (For Gov't. Agencies Use)
Columbus, OH	Director, DISCO, P.O. 2499 Columbus, OH 43216-5006	614 614	238-2133 (Duty Hrs.) 238-2058 (After Hrs.)	850-2133
Richmond, VA	Director, Department of Defense Security Institute, c/o DGSC Richmond, VA 23297	804	275-3012	695-3012
Brussels, Belgium	Physical Address: Director, OISI-E Steenweg OP Leuven 13, 1940 St. Stevens-Woluwe, Brussels, Belgium		322-725-0884	
	Mailing Address: Director, OISI-E APO New York 09667			
Mannheim, Germany	Chief, OISI Field Office Hammonds Barracks, APO New York 09333	(49621)	472582	380-8363
Seoul, Korea	Chief, OISI Field Office c/o EUSA APO San Francisco 96301	Seoul, Korea	0-822-7913-2409	293-2409

City & State	Address	Area Code	Telephone Number	AUTOVON NO. (For Gov't Agencies Use)
Yokohama, Japan	Physical Address: Room 211 and 213 Bldg. 200, North Dock, Yokohama, Japan Mailing Address: Chief, OIS1-FE/V0470 DIS, MTMCTY, FPO Seattle 98760	045-	441-0378	235-6703

Appendix IX. USE OF ESCORTS FOR CLASSIFIED SHIPMENTS

(also applies to carrier custodians)

A. General. Escorts must be cleared to the level of the information involved. A sufficient number of escorts shall be assigned to the classified shipment to ensure continuous surveillance and control over the shipment while it is in their custody.

B. Instructions and Operating Procedures. Specific written instructions and operating procedures will be furnished escorts prior to the shipment and should include, but not necessarily be limited to, the following:

1. general unclassified outline of the mission;

2. name and address of persons, including alternates, to whom the classified matter is to be delivered;

3. receipting procedures;

4. means of transportation to be used and route to be used;

5. duties of each escort during movement, during stops en route, and during loading and unloading operations; and

6. emergency and communication procedures.

C. Functions of An Escort. Escorts assigned for the protection of security shipments shall do the following:

1. Escorts shall conduct themselves throughout each security shipment operation in such manner that the security of matter entrusted to them will not be prejudiced through carelessness, inadvertence, or lack of vigilance. Intoxicants or drugs, which may impair their judgment, may not be used by escorts while assigned to a security shipment.

2. Escorts shall possess identification cards as prescribed in paragraph 8 and carry them at all times, while having custody of security shipments. These cards will be safeguarded, and the loss of a card will be reported immediately to their company security supervisors.

3. Escorts shall accept custody for the shipment by signing a receipt and release custody of the shipment to the consignee, after obtaining a receipt from one of the consignee's employees who has been positively identified and who is cleared to at least the same level as the classified shipment.

4. Escorts shall carry packages on their person, or in hand-carried containers, until they are delivered to the consignee, whenever practical. Such packages shall be kept under the constant surveillance of the escort who shall be in a physical position to exercise direct security controls over the material.

5. When accompanying classified material in an express or freight car, escorts shall provide continuous observation of the containers and observe adjacent areas during stops or layovers.

6. When traveling in an escort car accompanying a security shipment via rail, escorts shall keep the shipment cars under observation and detrain at stops, when practical and time permits, in order to guard the shipment cars and check the cars or containers locks and seals. The escort car (after appropriate arrangements with the railroad) should be prepositioned immediately behind the car used for the classified shipment, in order to enable the escort to keep the shipment car under observation.

7. Escorts shall maintain liaison, as required, with train crews, other railroad personnel, special police, and law enforcement agencies.

8. When escorting security shipments via motor vehicles, escorts shall maintain continuous vigilance for the presence of conditions or situations which might threaten the security of the cargo, take such action as circumstances might require to avoid interference with continuous safe passage of the vehicle, check seals and locks at each stop where time permits, and observe vehicles and adjacent areas during stops or layovers.

9. When escorting shipments via aircraft, escorts shall provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations. The escort shall not enplane until after the cargo area is secured. Furthermore, the escort should preferably be the first person to deplane in order to observe the opening of the cargo area. Advance arrangements with the airline are required.

10. Escorts shall notify the consignor by the fastest means available if there is an unforeseen delay en route, an alternate route is used, or an emergency occurs. If appropriate and the security of the shipment is involved, also notify the nearest office of the FBI.

Appendix X. REQUIREMENTS APPLICABLE TO THE HAND-CARRYING OF CLASSIFIED MATERIAL ABOARD COMMERCIAL PASSENGER AIRCRAFT

A. General. The following requirements apply to the hand-carrying of classified material aboard commercial passenger aircraft (also see paragraph 17). The hand-carrying of classified material aboard commercial passenger aircraft shall only be authorized after a determination has been made that: (i) a rare and unusual situation warrants such consideration, (ii) the essential classified material is not available at the destination point of the employee traveler, (iii) the material cannot be transmitted in sufficient time by other authorized means essential to accomplish the purpose of the visit, and (iv) the relative size, weight and physical configuration are such that the material may be carried on the traveler's person or otherwise qualify as carry-on baggage. Classified material shall not be hand-carried across international boundaries except on regularly scheduled nonstop flights on U.S. carriers between the U.S. Mainland and Alaska, Hawaii, Puerto Rico, or U.S. possessions or as otherwise provided for by this Manual.

B. Background. Federal Aviation Regulations require that all passengers and their carry-on items be screened prior to boarding scheduled passenger aircraft. The Department of Transportation, Federal Aviation Administration (FAA) Advisory Circular (AC 108-3), titled "Screening of Persons Carrying U.S. Classified Material," prescribes that individuals carrying classified materials shall be screened in the same manner as other passengers except when routine processing could subject the materials to compromise. If routine processing is not feasible, special processing procedures must be observed or the classified material may not be taken aboard the aircraft.

C. Routine Processing. Hand-held packages are normally screened by x-ray examination. Items concealed on the person are subject to other electronic screening devices. If by x-ray analysis, or any other method of security screening, an airline security agent suspects that a parcel or envelope may contain a weapon, explosive, incendiary, or dangerous object, the item must undergo further scrutiny or the prospective passenger will be denied the privilege of boarding with the material. As a general rule, however, contractor personnel hand-carrying classified material in sealed envelopes or small packages can be successfully processed by air carrier personnel at a screening station. To avoid unforeseen problems, it would be prudent if the employee carrying classified material possessed the identification and travel documentation described in paragraph E, below. Sound judgment should dictate whether such documentation need be prepared. When visual examination is or may be required to successfully screen a classified package, when routine x-ray examination could subject classified material to damage or compromise, or when other unusual circumstances exist, the special processing procedures of paragraph G, below, apply. However, under no circumstances may the classified material be opened by the employee traveler or air carrier personnel.

D. Approval. Classified material shall not be hand-carried aboard commercial passenger aircraft by contractor employees except as specified by paragraph 17c(3). Each approval to hand-carry shall be recorded and maintained by the FSO for a period of 2 years. However, the special authorization letter and company identification prescribed in paragraph E, below, is not required if the contractor has reason to believe that classified material can be routinely processed successfully through air carrier screening stations.

E. Authorization Letter and Identification Card. All contractor personnel utilizing the special screening procedures of paragraph G, below, must have written authorization to hand-carry classified material and possess a picture identification card or badge meeting the requirements of paragraph 8. If the traveler is the only employee assigned to a facility, or an air carrier has cause to authenticate the traveler's courier authorization, the CSO may be contacted to verify the authorization.

1. Traveling employees shall have the original written authorization (a reproduced copy is not acceptable). However, a sufficient number of authenticated copies must be available to provide a copy to each air carrier involved. The written authorization may contain a printed (or typed) endorsement for signature by the host security official at the destination if a round trip with classified material is foreseen. In addition, the written authorization shall:

a. be on letterhead stationery of the contractor authorizing the hand-carrying of classified material;

b. provide the full name, date of birth, height, weight, and signature of the traveler;

c. describe the type of identification the traveler will present on request (for example, ABC Corporation picture badge, No. 1234);

d. Describe the material being hand-carried which is requested to be exempt from opening (for example, three sealed packages, 9 1/2" x 12 1/2" x 2");

e. identify the points of departure, destination, and known transfer points;

f. be dated and have an expiration date which may not exceed 7 days from the date of issuance; and

g. carry the name, telephone number, title, and signature of the authorizing official and the name and telephone number of the facility's CSO.

2. The personal identification medium shall be an identification card badge, or credential issued by the contractor showing, as a minimum, the name and photograph of the employee traveler. The identification medium shall also carry the name of the employing contractor or otherwise be marked to denote "contractor."

3. When it appears an employee may be required to hand-carry classified material via commercial passenger aircraft on a return trip, and no endorsable letter of authorization from the employing contractor exists, it

will be necessary for an authorized security official at the activity being visited to determine whether further hand-carrying is essential. Depending on this determination, the host security official will: (i) provide a letter of authorization on the host's letterhead stationery, (ii) comply with the approval criteria prescribed in paragraph D, and (iii) make all other arrangements necessary for the hand-carry mission.

F. Preparation for Transmission. Classified material to be hand-carried shall be packaged as specified in paragraph 17 for material of the same level of classification except as follows:

1. The packaging, together with the classified material contained therein, shall, if possible, be of a thickness which facilitates physical inspection at the airport's passenger screening station by flexing, feeling, and weighing to preclude the need to visually examine the contents.

2. The packaging shall contain no bindings, paper clips, or other metal which would inhibit processing through detection devices at the airport.

3. Caution should be used in carrying film because x-ray equipment used to inspect carry-on items will damage certain types of high speed and sensitive film.

4. Any bulky item that requires screening will have a company shipping label affixed to the outer casing, shell, wrapper, or other covering. The label shall be signed by the same official who signed the letter of authorization.

G. Special Processing. Travelers carrying classified material aboard commercial passenger aircraft shall be processed through the air carrier ticketing and boarding procedure in the same manner as all other passengers except as follows:

1. If routine x-ray examination could subject the material to compromise or damage, perhaps by exposing film or revealing a classified configuration, the contractor shall notify an official of the appropriate air carrier in advance of the intended flight to explain the particular circumstances and obtain instructions as to the special screening procedures to be followed. The contractor should, if necessary, refer the air carrier official to FAA Advisory Circular 108-3. The employee will be required to produce company identification and proper authorization pursuant to paragraph E, above. If satisfied with the identification and letter of authorization, the carrier representative should provide the employee passenger with an escort to the screening station to authorize exemption of the classified material from inspection.

2. If during routine screening of classified carry-on baggage air carrier personnel are not satisfied with the results of the inspection, and the prospective passenger is requested to open a classified package for visual examination to overcome the impasse, the passenger shall: (i) inform the person conducting the screening that the pertinent carry-on items contain U.S. Government classified information and cannot be opened,

(ii) present company identification and proper authorization pursuant to paragraph E., above, (iii) refer the screening official to FAA Advisory Circular 108-3, and (iv) request special dispensation from the advance notification stipulation and ask that air carrier personnel telephonically contact the contractor or the CSO to verify the hand-carry authorization. The air carrier decision on such matters is final.

3. In rare instances, classified material may be in specialized containers which because of size, weight, or other physical characteristics may require special processing consideration. Under such unique circumstances, the procedures contained in paragraph 1, above, shall be followed.

4. On those occasions when a traveler does not have an authorization letter or company identification, and there is sufficient time prior to departure, the passenger may: (i) contact an air carrier ticket counter agent, (ii) explain the circumstances, (iii) produce acceptable alternative identification, and (iv) request special dispensation from the advance notification stipulation and ask that the air carrier telephonically contact the contractor authorizing official to verify the traveler's authorization to hand-carry classified material.

5. If the special processing procedures of paragraphs 1 thru 4, above, do not permit boarding with the classified package, the employee shall not proceed further and shall arrange with the facility for alternate means of transmitting the material. The passenger may not open or authorize the opening of these carry-on items under any circumstances. Any instances in which carry-on items have been opened shall be reported promptly to the FSO who shall report the matter to the CSO.

H. Incident Situations. Pursuant to this appendix, and in the event a contractor passenger is aboard a commercial passenger aircraft that is hijacked to a foreign country, the employee shall adhere to the following instructions:

1. Show appropriate civilian identification.

2. The employee shall not voluntarily reveal the existence of classified material nor draw attention to it.

3. If questioned or interrogated in a foreign country, common sense and judgment will be used in making any response. If prudent under the circumstances, the traveler shall attempt to maintain physical possession of the classified material at all times.

4. If, at any time, a classified package could not be maintained under the personal custody and control of the traveler, the package shall be provided, unopened, to the FSO upon return to the U.S.

5. On return to the U.S., the traveler shall immediately report the entire incident to the FSO who will report the matter to the CSO.

I. Briefing. The employees hand-carrying classified material aboard commercial passenger aircraft shall be briefed on their overall responsibility to safeguard classified material, on the contents of this appendix, and on the applicable portions of the contractor's SPP.

APPENDIX XI. INTRUSION DETECTION SYSTEM (IDS) REQUIREMENTS

A. Purpose. This appendix specifies the minimum standards for IDS equipment, installation, and operation when used to supplant guards required by paragraphs 14a and 34.

B. IDS Approval. Approval of the CSO is required before effecting the installation of an IDS to meet the requirements of this manual (see paragraph 34c regarding cost considerations).

C. IDS Equipment. All material, equipment, and sensors used in the IDS shall meet or exceed U.L. Standards as evidenced by a U.L. listing mark on such material, equipment or sensors. Manufacturers of U.L. listed equipment are contained in the U.L. Automotive, Burglary Protection and Mechanical Equipment Directory. Copies of this directory may be obtained from:

Underwriters Laboratories, Inc.
Publications Stock
333 Pfingsten Road
Northbrook, Illinois 60062

D. IDS Installation. The intrusion detection system at the protected facility, area or container shall be installed in accordance with U.L. Standards by a U.L. listed alarm installer or U.L. listed commercial central station. When connected to a commercial central station, the service provided must be Grade AA (response time to an activated alarm shall not exceed 15 minutes and the connecting lines are electronically supervised to detect evidence of tampering of malfunction). In environments where Grade AA service cannot be provided by a commercial central station due to such factors as traffic in highly congested urban areas or distance in remote rural areas, the CSO may authorize Grade BB service (20 minute maximum response with line supervision) or Grade CC service (30 minute maximum response time with line supervision), as appropriate. 1/ 2/ In all cases, the extent of protection for the premises shall be Installation Number 3 as specified on page 72 of the U.L. Automotive, Burglary Protection and Mechanical Equipment Directory.

E. Certification of Compliance. Evidence of compliance with paragraphs C and D, above, will consist of a valid (current) U.L. Certificate for the appropriate grade of service which has been issued to the protected facility by the commercial central station. In the case of a proprietary central supervising station, the U.L. listed company which installs the alarm issues the U.L. Certificate to the facility. The certificate serves as evidence that the installing company or commercial central station; (1) is listed as furnishing protecting systems of the class, type, and grade indicated; (2) is authorized to issue the certificate to the installation as its representation that the equipment is in compliance with requirements established by U.L. for the class; and, (3) is subject to the U.L. field countercheck program whereby periodic inspections are made of representative alarm installations by U.L. personnel to verify the correctness of certification practices. 3/

(Footnotes 1/ 2/ and 3/ are on the following page)

1/ The U.L. standard for response within the time limits set for the various grades of service (AA, BB, CC) is 80%. That is the minimum allowable on-time response rate. The 80% rate applies to all alarm installations where alarm systems are approved in lieu of guards as supplemental protection for classified information. Anything less than 80% is UNSATISFACTORY.

2/ In exceptional cases, where the requirements set forth in D, above, cannot be met due to extenuating circumstances, the contractor may request CSO approval for an alarm system connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station. The alarm system is activated and deactivated by employees of the contractor, but the alarm is monitored and responded to by personnel of the monitoring police organization. Such direct-connect systems may be requested only when: (i) the contractor facility is located in an area where commercial central station services are not available within the time constraints of Grades, AA, BB, or CC service; and, (ii) it is impractical for the contractor to establish a proprietary central supervising station. Nonetheless, installation of this type system must also be accomplished by a U.L. listed alarm installation company. Response time to a direct-connect alarm must not exceed 15 minutes from the time the alarm was first registered and arrangements must be made with the responding police department to immediately notify a representative of the contractor (preferably the FSO) on receipt of an alarm; and the representative of the contractor is required to report immediately to the facility to ascertain the nature of the alarm and to take appropriate measures to ensure the security of classified material. Approval of the CSO is required before the contractor may initiate or utilize a direct-connect system as an alternative to the use of a commercial central station or proprietary central supervising station. The installation proposal, explaining how the system would operate, must be submitted, in duplicate, to the CSO. The proposal must include sufficient justification for the granting of an exception and the full name and address of the police department that will monitor the system and provide required response. The name and address of the U.L. listed installer who installed the system and who will inspect, maintain and repair the equipment shall also be furnished.

3/ Cleared contractors may not install or certify their own proprietary alarm systems if those alarm systems are used to supplant the use of guards as supplemental controls (unless the cleared contractor in question is also a U.L. listed installer).

Appendix XII. DOCUMENTS ACCEPTABLE FOR PROOF OF U.S. CITIZENSHIP

A. A BIRTH CERTIFICATE indicating the individual was BORN IN THE UNITED STATES

B. A U.S. PASSPORT

C. A CERTIFICATE OF NATURALIZATION if the individual claims CITIZENSHIP BY NATURALIZATION

D. "A Report of Birth Abroad of a Citizen of the United States of America" (Form FS-240), a Certification of Birth (Form FS-545 or DS-1350), or a CERTIFICATE OF CITIZENSHIP if CITIZENSHIP WAS ACQUIRED BY BIRTH ABROAD TO U.S. CITIZEN PARENT OR PARENTS

E. If primary evidence of U.S. citizenship is not obtainable, then the best available secondary evidence, showing that the individual was born in the U.S., is required. Such evidence may include a combination of at least two of the following: a baptismal certificate; a hospital birth record; evidence of persons having personal knowledge of the facts of birth; or other documentary evidence, such as U.S. military records, early census, school or family Bible records, insurance papers, or newspaper files. The secondary evidence must be adequate to support a "good faith" determination that the individual is in fact a U.S. citizen. Secondary evidence submitted as proof of birth in the U.S. shall be original or certified documents. Noncertified copies are not acceptable.

The contractor will maintain a record as to which of the above documents were sighted as proof of citizenship.

Appendix XIII. GUIDANCE FOR CONTRACTOR SELF-INSPECTIONS

Each contractor is required to conduct a self-inspection program for evaluating all security procedures applicable to the facility's operation, in accordance with paragraph 5ac. As a minimum, a contractor self-inspection should include all elements normally inspected by the CSO. In order to assist the contractor in assessing the security posture of his or her facility, the following guideline questions used in part by CSO industrial security representatives are provided:

A. Facility Clearance.

1. Are the appropriate DD Forms 441, 441-1, and 441s on file (see paragraphs 21 and 73)?

2. Is the HOF/parent of the facility cleared or properly excluded (see paragraphs 72 and 73)?

3. Are all necessary OODEPs, directors or members of an executive *
committee appropriately cleared (see paragraph 22)? *

4. If all OODEPs are not cleared, have appropriate resolutions been furnished to the CSO (see paragraph 22e)?

5. Have changes in the information previously reported on DD Forms 441s been reported? (List changes which have occurred since the last inspection; see paragraph 6a(4)f.)

6. Have all changes affecting the FCL been reported to the CSO, for example, stock control, exclusion resolutions and changes of OODEPs (see paragraph 6a(4)f)?

7. Has a statement been submitted by each RFI (see paragraphs 6a(4), 6b(5), and 20k)?

B. Access Authorizations.

1. Are records maintained of clearances issued by the DoD and the facility, for example, records of DISCO Forms 560 and DD Forms 48-2 (see DISCO Form 560, DD Form 48-2, and paragraph 28)?

2. Are the number of clearances held to the minimum consistent with contractual requirements (see paragraph 20)?

3. Are clearance applications obtained and reviewed only after *
employment (see paragraph 25)?

4. Are all required information and forms furnished to DISCO (such as, adverse information, DISCO Form 562, DD Form 48-2, as applicable)? (Explain system and procedures for ensuring that adverse information is reported as required; see paragraphs 6b(1) and 24b.)

5. Are personnel transfers in an MFO reported to DISCO (see paragraph 26e)?

6. Are contractor CONFIDENTIAL clearances granted by a contractor's employee who is cleared by DoD (see paragraph 24a(1)(e))?

7. Have adequate procedures been established for the granting of CONFIDENTIAL clearances by the contractor (see paragraph 24b)?

8. Are review procedures in effect to preclude errors/omissions on clearance applications to DISCO (see paragraph 26a(3))?

9 Has the contractor elected to have LOC's issued to the HOF or to a PMF (see paragraph 26h(2)?

10. Has the election to have LOC's issued to the HOF or PMF been included in the SPP and approved by the CSO (see paragraph 73d)?

11. Are cleared employees (including immigrant aliens) assigned to overseas duty station for more than 90 consecutive days during any 12-month period? Is a report of such assignment submitted to DISCO (see paragraph 6b(6) and 96)?

C. Security Education.

1. Are procedures established for administering security briefings to cleared employees prior to granting access to classified information (see paragraph 5g)?

2. Is SF 312 or SF 189A (Classified Information Nondisclosure Agreement) executed as required (see paragraph 5g)? * *

3. Are refusals of employees to sign the Security Debriefing Acknowledgement (SF 312 or SF 189A) reported to DISCO or the CSO as required (see paragraph 6b(11))? * * *

4. Does the facility have an industrial security education program which includes recurring security indoctrination of its cleared employees? (Briefly explain how this program works; see paragraph 5f).

5. Does the contractor have a procedure for the conduct of a self-inspection of its complete security program (see paragraph 5ac)?

6. Has a procedure been established for evaluating the effectiveness of the self-inspection program? (Describe in the narrative the procedures used by the facility; see paragraph 5ac).

7. Is there an adequate procedure for ensuring personnel security administration and education for cleared personnel assigned to uncleared locations? (Describe in narrative the procedure used; see paragraph 73e).

8. Are special security briefings and debriefings given, and are records kept as required, for example, records pertaining to NATO and CNWDI (see paragraphs 85 and 119)?

9. Does management support the facility's security program (see paragraph 5aa)?

D. Standard Practice Procedure.

1. Is the SPP current and does it adequately implement ISM requirements as they apply to the facility operations? Has a copy been given to the CSO? (Provide date of SPP or of latest revision; see paragraph 5s).

2. Is the MFO or PMF SPP adapted to apply at operating locations (see paragraph 73a)?

E. Subcontracting.

1. Are the clearance status and safeguarding capability of the subcontractor determined as required (see paragraphs 58a and 59b)?

2. Is notification of selection of the subcontractor furnished to the contracting officer (see paragraph 62)?

3. Is written authority to disclose TOP SECRET information obtained from the contracting officer (see paragraph 59a)?

4. Is adequate classification guidance applicable to subcontracts extracted from the prime contract DD Form 254 and properly distributed to prospective or actual subcontractors (see paragraph 60a)?

5. Are DD Forms 254 pertaining to subcontractors approved by the contracting officer or, in the case of service contracts, by the prime contractor (see paragraph 60b)?

6. Is retention of classified information by subcontractors approved by the contracting officer (see paragraph 64)?

7. Are foreign classified subcontracts approved as required (see paragraph 65)?

F. Visit Control.

1. Is positive identification of visitors required and number of classified visitors held to a minimum (see paragraph 38a and 38b)?

2. Has action been taken to determine that the visiting contractor has been granted the appropriate FCL (see paragraph 38a)?

3. Are visitor records maintained, and do they contain required information (see paragraph 39)?

4. Are visitors escorted as required (see paragraph 38b)?

5. Are classified recordings, photos, and removal of classified material authorized as required (see paragraph 38c)?

6. Are classified visits by Category 4 visitors specifically approved by the UA (see paragraph 41d(1))?

7. Does the facility have proper procedures regarding Category 5 visitors; that is, briefings, debriefings, and reporting requirements (see paragraph 41e)?

8. Does the facility have long-term visitors? (If so, list by company those abiding by the host SPP and those using the SPP of their HOF's; see paragraph 40)

9. Are requests submitted in advance of visits and promptly canceled when required (see paragraph 37f)?

10. Is immediate notification regarding any change of individual or facility clearance status furnished to those activities which have received current visit requests (see paragraph 37f)?

11. Are requests to visit U.S. Government activities routed via the contracting officer when required (see paragraph 44)?

12. Are visit requests submitted to DISCO or OISI in connection with foreign visits as appropriate, and is sufficient lead time allowed (see paragraphs 48 and 49)?

13. Are NATO security clearance certificates furnished as requested (see paragraphs 52 and 55)?

G. Classification.

1. Is the facility furnished adequate classification guidance and notification of biennual review (see paragraphs 10a and 10b)?

2. Are security classifications, including downgrading and declassification instructions, applied to information in accordance with the applicable classification guidance (see paragraph 10f)?

3. Does the contractor challenge classification and marking guidance believed by him or her to be inadequate or erroneous (see paragraph 10e)?

4. Is security classification marking by the contractor supported by adequate records (see paragraph 10f)?

5. Is the number of employees authorized to be responsible for the currency, necessity, and accuracy of applied security classifications held to a minimum (see paragraph 10f(4))?

6. Are security classification guidance and marking instructions adequately disseminated within the facility (see paragraphs 10f and h)?

7. Are downgrading and declassification actions taken in accordance with established schedules (see appendix II)?

8. Are adequate classification guidance and marking instructions furnished in connection with foreign classified contracts (see paragraph 11e)?

H. Employee Identification.

1. Are badges and identification cards properly controlled; do they contain the required data (see paragraph 8a)?

2. Are badges and/or cards designed to minimize tampering; are they properly constructed (see paragraph 8a(4))?

3. Are new or revised badge or card systems reported to the CSO (see paragraph 8c)?

4. Are visitor badges properly controlled (see paragraph 8b)?

5. How many badges and identification cards are lost or out of control? What percent of the total issued? How long has current system been in effect (no reference)?

6. Are badges and/or cards recovered as required (see paragraph 8a(5))?

I. Foreign Contacts/Travel.

1. Are reports of personal exchanges with nationals or represent- *
atives of Designated countries, foreign travel or attendance at inter- *
national meetings submitted to DISCO as required (see paragraph 6b(9)? *

2. How many reports were submitted since the last inspection (see paragraph 5u)?

3. Are briefings given as required, and briefing forms retained for the required period of time (see paragraph 5u(2))?

4. Is classified information accounted for prior to each employee's departure (see paragraph 5u)?

5. Have representatives of Designated countries visited the facility since the last inspection, and what special security measures and briefings were utilized in preparation? Were any problems encountered? (Explain fully in narrative; see paragraphs 5o, 5u, and 6a(19)).

J. Public Release.

1. Is public release of information pertaining to classified contracts approved by the appropriate U.S. Government activity? (Indicate the number of approved releases since last inspection, including contract number, nature of release, and identification of approving authority; see paragraph 5o).

2. Is classified sales literature approved by contracting officer prior to publication and distribution (see paragraph 5p)?

3. Is authorization for publication and distribution indicated on the cover or the first page of document (see paragraph 5p)?

K. Classified Storage.

1. Are containers kept locked, when not under direct and continuous surveillance by an authorized person (see paragraph 14c)?

2. Are the number of persons possessing knowledge of the combinations or having access to contents of containers held to a minimum (see paragraph 14c)?

3. When combinations to classified containers are placed in written form, are they properly marked, stored, and accounted for (see paragraph 5i)?

4. Are combinations changed by an authorized person (see paragraph 5i)?

5. Are combination padlocks properly protected when the container is open (see paragraph 5i)?

6. Are steel bars affixed to file cabinets in such a manner to preclude surreptitious removal of classified information (see paragraph 14a(3)(d), footnote 10)?

7. Are adequate supplemental controls established where required? (Completely describe supplemental controls in effect at the time of inspection. Fully identify those controls that are established for security containers and those established for controlled areas. See question 9 below; see paragraphs 14a(2) and (4)).

8. Are vaults and strongrooms properly constructed (see appendix IV)?

9. Is classified waste properly protected (see paragraph 19f)?

10. Does the facility use alternate storage locations? (If so, give full details, to include contracting officer's approval and location; see paragraph 15).

11. Are security checks performed to ensure that classified material is protected at all times (see paragraph 5j)?

12. Does the CSO have inspection responsibility for all classified material and areas? (If not, give particulars as to how the CSO was relieved of inspection responsibility and for what specific areas.)

L. Markings.

1. Are classified hardware and documents properly marked (see paragraph 11)?

2. Are the date of origin and the name and address of the facility responsible for preparation placed on documents (see paragraph 11b(1))?

3. Are portions of classified documents properly marked (see paragraph 11b(5))?

4. Are all additional markings applied as required (see paragraph 11b(8))?

5. Is foreign classified information marked with U.S. equivalent classification marking (see paragraph 11e)?

6. Are rolled and/or folded documents marked as required (see paragraph 11c(2))?

7. Are downgrading/declassification notations properly assigned and completed (see paragraph 11b(7) and appendix II)?

M. Transmissions.

1. Is classified information properly prepared and transmitted outside and within the facility (see paragraph 17)?

2. Are the FCL and safeguarding capability determined prior to dispatch of classified information to other contractors (see paragraphs 58 and 59)?

3. Are messengers that handle classified material properly cleared (see paragraph 17c(3))?

4. If vehicles are used for the delivery of classified material, is the material kept under the constant surveillance of an appropriately cleared employee (see paragraph 17h)?

5. Are procedures established and implemented for the proper receipt of classified material by the facility (see paragraph 12e)?

6. Is written authorization for the transmittal of TOP SECRET information obtained from the contracting officer (see paragraph 17b)?

7. Is export of U.S. classified material approved and accomplished on a government-to-government basis (see paragraph 17e)?

8. Is the transmittal of classified information outside the U.S., Puerto Rico, or a U.S. possession or trust territory properly accomplished (see paragraph 17e)?

9. Are classified shipments made only in accordance with the ISM or instructions from the contracting officer (see paragraph 17c(5))?

10. Is consignee given an advance notice of classified shipment (see paragraphs 17d(3)(d) and 17c(5)(d))?

11. Is the CSO notified of overdue classified shipments (see paragraphs 17d(3)(d) and 17c(5)(d))?

12. Are classified shipments properly inspected on receipt (see paragraphs 12 and 17)?

13. Is classified information, which is hand-carried in connection with visits, properly approved in advance, accounted for, and stored (see paragraph 17i)?

14. Are procedures established to preclude transmission of classified information via unapproved communication circuits (see paragraph 17c(4))?

15. Is a suspense system maintained of receipts for classified transmittals, and is adequate follow-up action taken, if receipts are not returned (see paragraph 12g(3))?

16. Are procedures established for the hand-carrying of classified material, for example, by commercial aircraft, (see paragraph 17 and appendix X)?

N. Classified Material Controls.

1. Have control stations been established? Indicate the number of master stations and substations (see paragraph 12a).

2. Are complete records kept for classified material received and dispatched outside of the facility (see paragraphs 12a and 12c)?

3. Is accountability maintained for all TOP SECRET, SECRET, and CRYPTO materials, including documents, hardware, and mock-ups, to permit their prompt location (see paragraphs 12a and 12f(3))?

4. Are accountability and receipt and dispatch records retained for the required time (see paragraphs 12a, 12c, and 19e)?

5. Are procedures established for accountability of TOP SECRET and SECRET working material that is not promptly destroyed as classified waste (see paragraph 12f)?

6. Are control station personnel cleared to the appropriate level and knowledgeable of their responsibilities (see paragraph 5f and 12d)?

7. Is a system in place to deter and detect the unauthorized *
introduction or removal of classified material from the facility (see *
paragraph 5am for perimeter controls)? *

8. Are procedures established to ensure prompt reporting to the FSO and investigation of each loss, compromise, or suspected compromise of classified material and other security violations. (Indicate number of occurrences since last inspection; see paragraphs 6a(2), 6a(3) and 7.)

9. Is an annual inventory and accounting made of TOP SECRET material? (Indicate date of last inventory; see paragraphs 12b and 13h).

10. Are TOP SECRET documents controlled by access records, continuous receipt system, number series, and copy numbers (see paragraph 13)?

11. Is access to classified material controlled on a need-to-know basis (see paragraph 3bg and 5c)?

12. Are adequate procedures implemented to fully ensure the safeguarding of classified material during its use (see paragraphs 5c, 5d, and 16)?

O. Controlled Areas.

1. Are closed areas properly constructed (see paragraph 34a and appendix v)?

2. Are areas properly posted and approved by the CSO (see paragraphs 34a(4), 34b(3), and 34c)?

3. Are area entrances properly controlled, and is admittance granted on a need-to-know basis (see paragraph 34)?

4. Are employees assigned to areas instructed to challenge unknown persons in areas (see paragraph 34a(5))?

5. Is movement of classified material to and from areas properly supervised (see paragraph 34a(2))?

6. Are employee badges, cards, or access lists properly controlled and kept current (see paragraphs 8a(5) and 34)?

7. Are visitors to areas properly controlled (see paragraphs 8b, 32, and 34a)?

8. Are supplanting electromechanical access control devices properly regulated (see paragraph 36a)?

9. Are guard patrols or supplanting intrusion detection systems adequate for closed areas during nonworking hours (see K-7 above and paragraphs 33b, 34a(3), 35, and 36)? *

10. Are cleared, trained alarm monitors in attendance at the station at all times when the IDS is in operation (see paragraph 35a(1)(c))? *

11. Are records properly maintained as required by paragraph 35h and *
35j? *

12. Are IDS immediately activated at the close of business (see *
paragraph 35a(1)j? *

13. Is the response time to an activated alarm 15 minutes or less or *
as otherwise required by the UL certification which was approved by the CSO? *
(See appendix XI, paragraph D.)

14. Does material, equipment, and installation of the IDS meet UL specifications? (See appendix XI, paragraphs C and D.) *

P. Disposition.

1. Is a program established for the reduction of classified holdings (see paragraph 19a)?

2. Is classified material (including waste) destroyed as soon as practical (see paragraph 19a and 19c)?

3. Is classified material properly destroyed (that is, does destruction process preclude reconstruction; see paragraphs 19c and 19f)?

4. Is burning the only approved method of destruction used by the facility? (List methods of destruction, other than burning, which have been approved by CSO; see paragraph 19c).

5. Are destruction records and certificates maintained as required (see paragraph 19e)?

6. Is destruction authority obtained when required (see paragraph 19b)?

7. Is destruction performed and witnessed by appropriately cleared personnel who are knowledgeable of their responsibilities (see paragraph 19d)?

8. Is destruction equipment leased or rented (see paragraph 19c)?

9. If the answer to 8 is "yes," who operates the equipment, and how is control of the material maintained (see paragraph 19c)?

10. Are procedures in effect to prevent access by uncleared employees who operate equipment (see paragraph 19c and 19g)?

11. Is retention authority requested on final delivery of goods or services or on complete termination of contract? (Explain how procedures are verified and how facility accomplishes this; see paragraph 5m.)

Q. Reproduction.

1. Is reproduction held to the minimum required? Are reproduction facilities properly designated, identified, and controlled (see paragraph 18)?

2. Are procedures in effect to restrict use of office reproduction equipment for classified productions? (If so, explain; see paragraph 18.)

3. Has the facility developed a procedure for the use of office copy machines in the reproduction of classified material (see paragraph 18)?

4. Are personnel thoroughly familiar with and following established procedures when using office copy machines for reproduction of classified material (see paragraphs 5f and 18)?

5. Is reproduction authorization obtained when required (see paragraph 18a)?

6. Are reproduction records properly maintained (see paragraph 18c)?

7. Are production control records properly maintained (see paragraph 78)?

8. Are copies or extracts of classified material marked the same as originals (see paragraphs 18 and 18d)?

9. Do reproduction area controls prevent unauthorized access (see paragraph 79)?

10. Are overruns held to a minimum and properly accounted for (see paragraph 80a)?

11. Are proofs and samples returned to the customer with finished products (see paragraphs 80b and 80d)?

12. Are classified waste containers identified and emptied at completion of working hours (see paragraph 80c)?

13. Are plates and rubber blankets reused only on classified production and safeguarded when not in use (see paragraph 80f)?

14. Are press rollers, and similar devices, properly cleaned after classified run (see paragraph 80f)?

15. Are mailing lists properly protected (see paragraph 82)?

R. Classified Meetings.

1. Are meetings sponsored when required? Indicate the number of meetings since last inspection (see paragraphs 5q(2), 5q(3), and 9).

2. Is attendance of foreign nationals or RFI's approved by sponsoring activity (see paragraph 9b)?

3. Are classified meetings held at approved locations (see paragraph 9c)?

4. Has the contractor developed complete security procedures for the safeguarding of classified material at the meeting (see paragraph 9d)?

5. Have the security procedures been submitted to the sponsoring activity for approval (see paragraph 9d)?

6. Is attendance limited to persons properly cleared and having a need-to-know (see paragraph 9d(1)(a))?

7. Is disclosure authority obtained from the contracting officer when required, and is disclosure authority furnished to sponsoring activity (see paragraph 9e)?

8. Is a copy of the classified presentation furnished to sponsoring and contracting activity (see paragraph 9e)?

9. Are unsponsored contractor-conducted meetings properly controlled (see paragraph 5q(1))?

10. Are requests to attend meetings properly certified and submitted to contracting officer UA activity for certification of the employee's need-to-know (see paragraph 9f)?

S. Consultants.

1. Are Type A Consultants properly briefed and certificates furnished to CSO? Are all necessary reports including adverse information reports, made as necessary, and on a timely basis (see paragraph 68)?

2. Are Type C Consultants properly briefed, and are controls stated in letter agreements observed (see paragraph 70)?

T. AIS.

1. Does the facility process classified information on an AIS system? (If so, what level?)

2. Has an AIS system security supervisor been appointed? (If so, identify by name; see paragraph 103c.)

3. Has written approval been given by the CSO to operate the system? (If "yes," list date of approval; see paragraph 103b.)

4. Have AIS hardware configurations, system software, or operating procedures/mode changed or been modified since the last inspection? (If "yes," give detailed explanation; see paragraphs 103b and 106a.)

5. Is the AIS SPP current? (If "yes," give date of issue; see paragraph 112d.)

6. Have the following provisions of section XIII, ISM, been satisfactorily implemented in the operation of the AIS?

a. Personnel controls (see paragraph 105)?

b. Physical controls (see paragraph 106)?

c. Clearance/declassification/destruction of all storage media (see paragraphs 114, 115, and 116)?

d. Transmission line protection (see paragraph 109)?

e. Subcontracting provisions (see paragraph 110)?

f. Audit trails, logs, and activity and maintenance records (see paragraph 111)?

U. COMSEC/CRYPTO.

1. Has a COMSEC custodian been appointed? (If so, list name and telephone number; see paragraph 12a, CSISM.)

2. Has an alternate COMSEC custodian been appointed? (If so, list name and telephone number; see paragraph 12a, CSISM.)

3. If appointed, are the COMSEC custodian and the alternate thoroughly familiar with and performing the duties outlined for them in the CSISM (see paragraph 18a, CSISM)?

4. Has a COMSEC account number been assigned? (If so, list the account number.)

5. What is the highest level of COMSEC access required? (Check one: ____TS____S____C)

6. Is COMSEC access required at the facility? (Briefly describe the type of access, for example, install, maintain, or operate COMSEC or CRYPTO equipments for the U.S. Government; operate communications link with the U.S. Government; have access to the operational keying variables; and manufacture or installation of keying material for COMSEC equipments.)

7. Does the facility have access to classified COMSEC information at another location (see paragraph 10, CSISM)?

8. List the number of employees who are briefed for access to COMSEC information (see paragraphs 10a and 11, CSISM).

9. Have employees authorized access to classified COMSEC information been properly briefed by U.S. Government representatives and/or contractor personnel (see paragraph 10, CSISM)?

10. Does the facility have a CSISM and applicable equipment doctrine?

11. Does the facility SPP contain adequate procedures relative to COMSEC requirements (see paragraph 1e, CSISM)?

12. Are all COMSEC related reports submitted (see Section XVI, CSISM)?

13. Has a COMSEC emergency plan been developed, which has the approval of the CSO (see paragraph 103, CSISM)?

14. Has adequate classification guidance been furnished regarding COMSEC information via a DD Form 254 (see paragraph 1b, CSISM)?

15. Have all disclosures of COMSEC information, whether to a subcontractor or other persons, been made only with the specific written approval of the contracting officer (see paragraph 75, CSISM)?

16. Is all COMSEC information in the custody of the facility properly marked and accounted for (see paragraph 12, CSISM)?

17. Are COMSEC and keying materials marked CRYPTO properly stored? (Describe the type of storage facilities used whether GSA container, vault, or other; see paragraph 90, CSISM.)

18. Are COMSEC and keying materials marked CRYPTO properly handled in the work processing area(s)? (If areas are utilized, briefly describe the characteristics of the area(s); see paragraph 88, CSISM.)

19. Are access lists properly posted (see paragraph 88, CSISM)?

20. Are adequate supplemental controls utilized, if necessary? (Describe them; see paragraphs 88 and 90, CSISM.)

21. Is COMSEC and CRYPTO material properly disposed of? (Describe what methods of destruction and disposition are used; see Section XIV, CSISM.)

22. Does the facility operate a communications center for the U.S. Government? Does it secure a communications circuit with the U.S. Government, or between itself and another contractor (see paragraph 1, CSISM)?

23. Are COMSEC and keying materials marked "CRYPTO" properly transmitted outside the facility (see paragraph 55, CSISM)?

V. International Operations.

1. Does the contractor have any cleared personnel assigned overseas? If so, are they doing any of the following?

a. Are they performing on a UA contract involving access to classified information overseas? (If "yes," include the number of personnel, the location of their work, and a list of contract number(s).)

b. Are they performing on an FMS contract involving access to U.S. classified information? (If "yes," indicate whether the access is provided directly to contractor personnel overseas by a U.S. Government activity, or if it is provided directly to contractor personnel by the foreign government for whom the FMS contract was awarded.)

c. Are they performing on a purely commercial contract awarded directly by the foreign government or one of its contractors, and access to either foreign classified or U.S. classified information is involved? (If

best copy available

"yes" and access is to U.S. classified information, determine how the U.S. classified information was released to the foreign government, such as, released directly by result of an export license, released by a third country with U.S. Government approval, and the like.)

d. Are they engaged exclusively in sales and marketing activities? (If "yes," identify what programs involve access to U.S. classified information and what the authority is for discussing such classified sales and marketing efforts with foreign nationals, such as U.S. Government approval, export licenses, and trade agreements.)

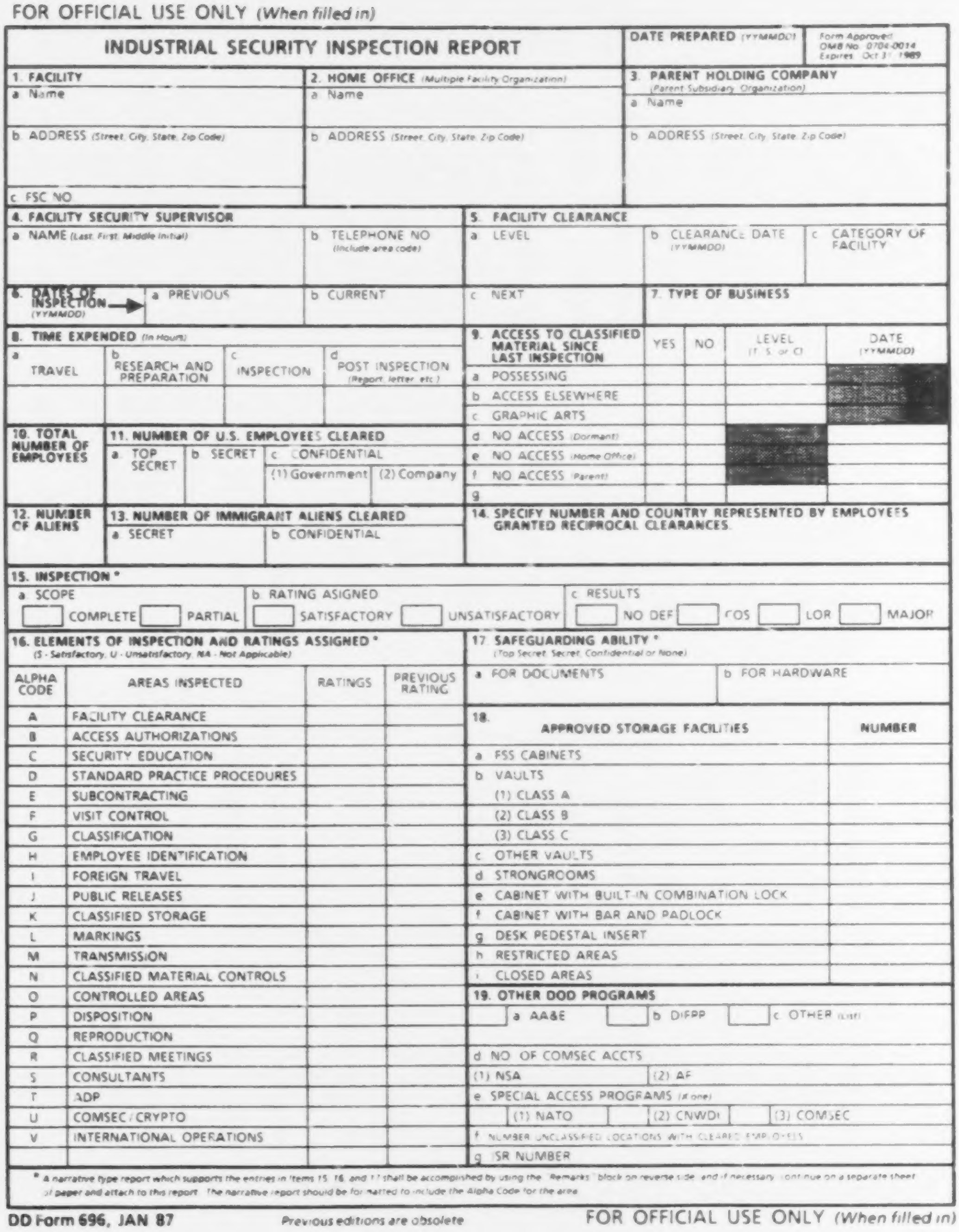
2. Has the contractor developed an SPP sufficient to cover its overseas operations when engaged in: (a) sales and marketing efforts involving U.S. classified information, and/or (b) performance on a UA awarded classified contract, including those contracts awarded under FMS? Does the SPP state the prohibition against contractors transporting classified material across international borders (see paragraph 5s)?

3. How many cleared employees are assigned overseas, and have they received the required security briefing prior to overseas assignment? Are there provisions for ensuring that employees receive an annual refresher briefing? (Explain the procedures established for ensuring that an annual refresher briefing is given; see paragraph 97.)

4. Has the contractor established a program for self-inspection of its overseas locations when the overseas location is engaged in work requiring access to either U.S. classified information or foreign classified information released to the contractor through U.S. Government channels? (Explain fully in the narrative the procedures established; see paragraph 97.)

SAMPLE

DD Form 696



FOR OFFICIAL USE ONLY *(When filled in)*

INDUSTRIAL SECURITY INSPECTION REPORT

DATE PREPARED *(YYMMDD)*

Form Approved
OMB No. 0704-0014
Expires Oct 31 1989

1. FACILITY	**2. HOME OFFICE** *(Multiple Facility Organization)*	**3. PARENT HOLDING COMPANY** *(Parent Subsidiary Organization)*
a Name	a Name	a Name
b ADDRESS *(Street, City, State, Zip Code)*	b ADDRESS *(Street, City, State, Zip Code)*	b ADDRESS *(Street, City, State, Zip Code)*
c FSC NO		

4. FACILITY SECURITY SUPERVISOR		**5. FACILITY CLEARANCE**		
a NAME *(Last, First, Middle Initial)*	b TELEPHONE NO *(Include area code)*	a LEVEL	b CLEARANCE DATE *(YYMMDD)*	c CATEGORY OF FACILITY
6. DATES OF INSPECTION → *(YYMMDD)* a PREVIOUS	b CURRENT	c NEXT	**7. TYPE OF BUSINESS**	

8. TIME EXPENDED *(In Hours)*

a TRAVEL	b RESEARCH AND PREPARATION	c INSPECTION	d POST INSPECTION *(Report, letter, etc.)*

9. ACCESS TO CLASSIFIED MATERIAL SINCE LAST INSPECTION	YES	NO	LEVEL *(T, S, or C)*	DATE *(YYMMDD)*
a POSSESSING				▨
b ACCESS ELSEWHERE				▨
c GRAPHIC ARTS				▨
d NO ACCESS *(Dormant)*			▨	
e NO ACCESS *(Home Office)*			▨	
f NO ACCESS *(Parent)*			▨	
g				

10. TOTAL NUMBER OF EMPLOYEES	**11. NUMBER OF U.S. EMPLOYEES CLEARED**			
	a TOP SECRET	b SECRET	c CONFIDENTIAL (1) Government	(2) Company

12. NUMBER OF ALIENS	**13. NUMBER OF IMMIGRANT ALIENS CLEARED**	
	a SECRET	b CONFIDENTIAL

14. SPECIFY NUMBER AND COUNTRY REPRESENTED BY EMPLOYEES GRANTED RECIPROCAL CLEARANCES.

15. INSPECTION *

a SCOPE ☐ COMPLETE ☐ PARTIAL

b RATING ASIGNED ☐ SATISFACTORY ☐ UNSATISFACTORY

c RESULTS ☐ NO DEF ☐ COS ☐ LOR ☐ MAJOR

16. ELEMENTS OF INSPECTION AND RATINGS ASSIGNED *
(S - Satisfactory, U - Unsatisfactory, NA - Not Applicable)

ALPHA CODE	AREAS INSPECTED	RATINGS	PREVIOUS RATING
A	FACILITY CLEARANCE		
B	ACCESS AUTHORIZATIONS		
C	SECURITY EDUCATION		
D	STANDARD PRACTICE PROCEDURES		
E	SUBCONTRACTING		
F	VISIT CONTROL		
G	CLASSIFICATION		
H	EMPLOYEE IDENTIFICATION		
I	FOREIGN TRAVEL		
J	PUBLIC RELEASES		
K	CLASSIFIED STORAGE		
L	MARKINGS		
M	TRANSMISSION		
N	CLASSIFIED MATERIAL CONTROLS		
O	CONTROLLED AREAS		
P	DISPOSITION		
Q	REPRODUCTION		
R	CLASSIFIED MEETINGS		
S	CONSULTANTS		
T	ADP		
U	COMSEC/CRYPTO		
V	INTERNATIONAL OPERATIONS		

17. SAFEGUARDING ABILITY *
(Top Secret, Secret, Confidential or None)

a FOR DOCUMENTS	b FOR HARDWARE

18. APPROVED STORAGE FACILITIES	NUMBER
a FSS CABINETS	
b VAULTS	
(1) CLASS A	
(2) CLASS B	
(3) CLASS C	
c OTHER VAULTS	
d STRONGROOMS	
e CABINET WITH BUILT-IN COMBINATION LOCK	
f CABINET WITH BAR AND PADLOCK	
g DESK PEDESTAL INSERT	
h RESTRICTED AREAS	
i CLOSED AREAS	

19. OTHER DOD PROGRAMS

☐ a AA&E ☐ b DIFPP ☐ c OTHER *(List)*

d NO. OF COMSEC ACCTS

(1) NSA (2) AF

e SPECIAL ACCESS PROGRAMS *(If one)*

☐ (1) NATO ☐ (2) CNWDI ☐ (3) COMSEC

f NUMBER UNCLASSIFIED LOCATIONS WITH CLEARED EMPLOYEES

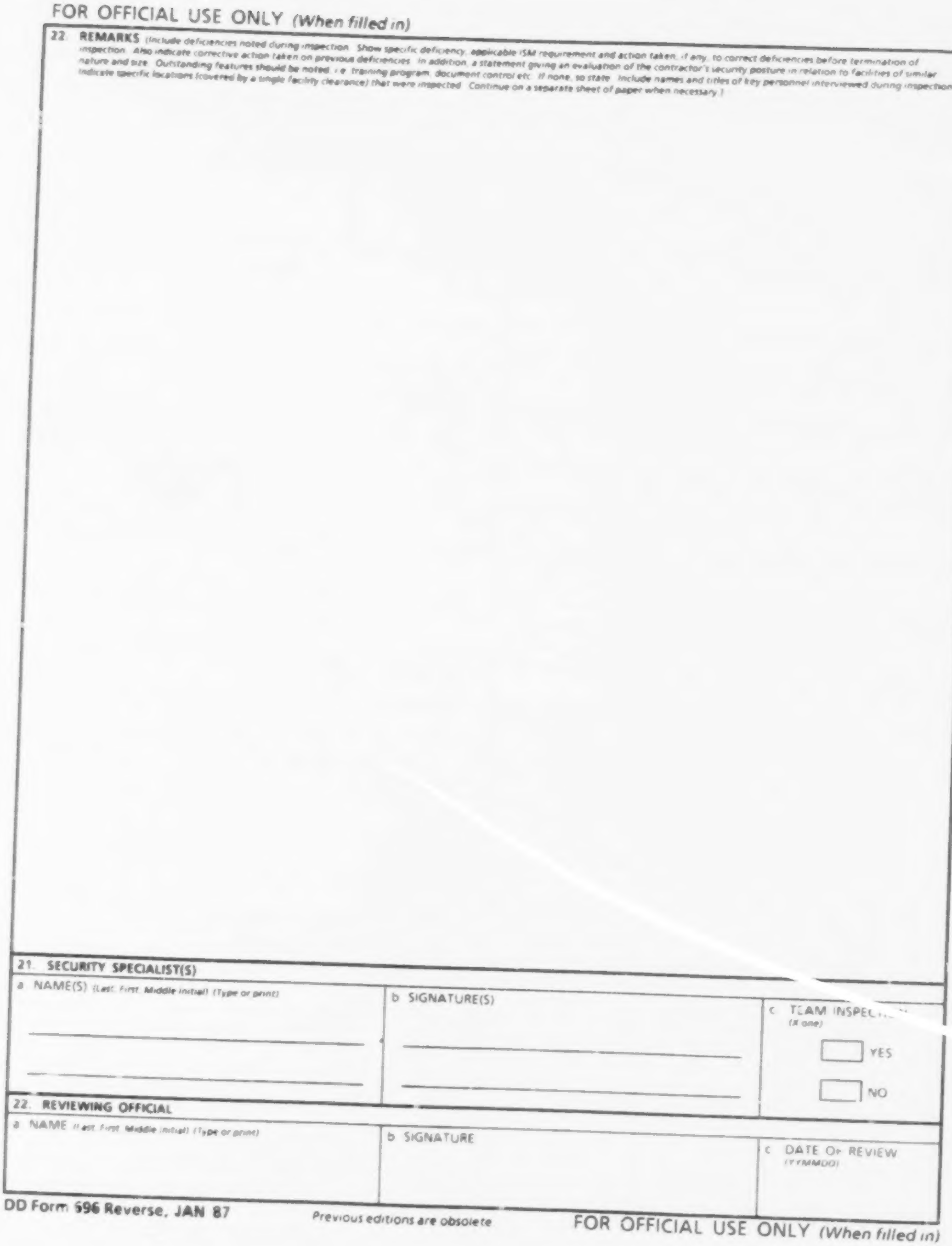
g ISR NUMBER

* *A narrative type report which supports the entries in Items 15, 16, and 17 shall be accomplished by using the "Remarks" block on reverse side, and if necessary, continue on a separate sheet of paper and attach to this report. The narrative report should be formatted to include the Alpha Code for the area.*

DD Form 696, JAN 87 *Previous editions are obsolete* FOR OFFICIAL USE ONLY *(When filled in)*

SAMPLE

DD Form 696
Page Two



FOR OFFICIAL USE ONLY *(When filled in)*

22. **REMARKS** *(Include deficiencies noted during inspection. Show specific deficiency, applicable ISM requirement and action taken, if any, to correct deficiencies before termination of inspection. Also indicate corrective action taken on previous deficiencies. In addition, a statement giving an evaluation of the contractor's security posture in relation to facilities of similar nature and size. Outstanding features should be noted, i.e. training program, document control etc. If none, so state. Include names and titles of key personnel interviewed during inspection. Indicate specific locations (covered by a single facility clearance) that were inspected. Continue on a separate sheet of paper when necessary.)*

21. **SECURITY SPECIALIST(S)**

a. NAME(S) *(Last, First, Middle initial) (Type or print)*	b. SIGNATURE(S)	c. TEAM INSPEC *(X one)* ☐ YES ☐ NO

22. **REVIEWING OFFICIAL**

a. NAME *(Last, First, Middle initial) (Type or print)*	b. SIGNATURE	c. DATE OF REVIEW *(YYMMDD)*

DD Form 696 Reverse, JAN 87 *Previous editions are obsolete* FOR OFFICIAL USE ONLY *(When filled in)*

APPENDIX XIV
Equivalent Foreign and International Pact Organization Security Classifications

Country	TOP SECRET	SECRET	CONFIDENTIAL	Non-U.S. Protective Classification Markings
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERTKE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Cambodia	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	SECRETO	RESERVADO	RESERVADO
Columbia	ULTRASECRETO	SECRETO	RESERVADO	CONFIDENCIAL RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENCIAL	
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO

Country	TOP SECRET	SECRET	CONFIDENTIAL	Non-U.S. Protective Classification markings
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Ethiopia	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN	SALAINEN		
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	VS—NUR FÜR DEN DIENSTC BRACH (VS—NFD)
Greece	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ	ΑΠΟΡΡΗΤΟΝ	ΕΜΠΙΣΤΕΥΤΙΚΟΝ	ΠΕΡΙΩΡΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ
Guatemala	ALTO SECRETO	SFCRETO	CONFIDENCIAL	RESERVADO
Haiti		SECRET	CONFIDENTIAL	
Honduras	SUPER SCERETO	SECRETO	CONFIDENCIAL	RESERVADO
Hong Kong	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Hungary	SZIGORÚAN TITKOS	TITKOS	BIZALMAS	
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS	
Iran	BEKOLI SERRI بکلی سری	SERRI سری	KHEILI MAHRAMANEH خیلی محرمانه	MAHRAMANEH محرمانه
Iraq	سري بلقوة (Absolutely secret)	سري (Secret)	مكتوم	محدود (Limited)
Iceland	ALGJORTI	TRUNADARMAL		

Country	TOP SECRET	SECRET	CONFIDENTIAL	Non-U.S. Protective Classification Markings
Ireland Gaelic	TOP SECRET AN-SICREIDEACH	SECRET SICREIDEACH	CONFIDENTIAL RUNDA	RESTRICTED SRIANTA
Israel	SODI BEYOTER סודי ביותר	SODI סודי	SHAMUR שמור	MUGBAL מוגבל
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	KIMITSU 機密	GOKUHI 極密	HI 秘	TORIATSUKAICHUI 取扱注意 BUGAIHI 部外秘
JORDAN	مكتوم جداً MAKTUM JIDDAN	سري MAKTUM	مكتوم SIRRI	محدود MAHDUD
Korea	Ⅰ급 비밀 I KUP PI MIL	Ⅱ급 비밀 II KUP PI MIL	Ⅲ급 비밀 III KUP PI MIL	
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Lebanon	TRES SECRET	SECRET	CONFIDENTIEL	
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
Netherlands	ZEER GEHEIM	GEHEIM	CONFIDENTIEEL or VERTROUWELIJK	DIENSTGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENEIELT	BEGRENSET
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENCIAL	RESERVADO

Country	TOP SECRET	SECRET	CONFIDENTIAL	Non-U.S. Protective Classification Markings
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Saudi Arabia	Saudi Top Secret	Saudi Very Secret	Saudi Secret	Saudi Restricted
Singapore	Top Secret	Secret	Confidential	*Restricted
Spain	MAXIMO SECRETO	SECRETO	CONFIDENCIAL	DIFFUSSION LIMITADA
Sweden (Red Borders)	HEMLIG	HEMLIG	HEMLIG	
Switzerland	(Three languages. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL.)			
French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
German	STRENG GEHEIM	GEHEIM	VERTRAULICH	
Italian	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Taiwan	絕對機密	極機密	機密	密
Thailand	LUP TISUD ลับที่สุด	LUP MAAG ลับมาก	LUP ลับ	POK PID ปกปิด
Turkey	ÇOK GİZLİ	GİZLİ	ÖZEL	HIZMETE ÖZEL
Union of South Africa				
English	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Afrikaans	UITERS GEHEIM	GEHEIM	VERTROULIK	BEPERK
United Arab Republic (Egypt)	سري للغاية TOP SECRET	سري جداً VERY SECRET	سري SECRET	محصور OFFICIAL

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	NON-U.S. PROTECTIVE CLASSIFICATION MARKINGS
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
USSR	**СОВЕРШЕННО СЕКРЕТНО**	**СЕКРЕТНО**	**НЕ ПОДЛЕЖАЩИЙ ОГЛАШЕНИЮ**	**ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ**
Viet Nam				
French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Vietnamese	TỐI-MẬT	MẬT	KIN	TU MẬT

INTERNATIONAL ORGANIZATION	TOP SECRET	SECRET	CONFIDENTIAL	
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED

NOTES:

In all instances foreign security classification systems are not exactly parallel to the U.S. system and exact equivalent classifications cannot be stated. The classifications given above represent the nearest comparable designations that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classifications.

"ATOMAL" information is an exclusive designation used by NATO to identify RESTRICTED DATA or FORMERLY RESTRICTED DATA information released by the U.S. Government to NATO.

There is no Swedish security classification equivalent to U.S. CONFIDENTIAL. Accordingly, all Swedish information or material received by the U.S. Government and classified HEMLIG will be safeguarded as U.S. SECRET; U.S. information or material received by the Swedish Government and classified CONFIDENTIAL will be safeguarded as HEMLIG.

*Singapore Restricted Information is protected as FOUO.

Appendix XV. AREAS COVERED BY MTMC AND HOTLINE NUMBERS TO BE USED FOR EMERGENCIES

The Bill of Lading of each shipment of classified material by a Commercial Carrier must contain the HOTLINE telephone number for the appropriate MTMC area. The areas covered and the HOTLINE numbers for the two commands are as follows:

EASTERN AREA

Alabama, Arkansas, Connecticut, Delaware, District of Columbia, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, West Virginia, and Wisconsin.

Address

Commander, Military Traffic
Management Command
Eastern Area ATTN: MTE-IN
Bayonne, NJ 07002

Telephone No.

Commercial No: 201-858-6566
Autovon: 247-6566 *
HOTLINE No: 800-524-0331

New Jersey only: 201-823-5323 *
800-624-1361 *

WESTERN AREA

Arizona, California, Colorado, Idaho, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oregon, South Dakota, Utah, Washington, and Wyoming.

Address

Commander, Military Traffic
Management Command
Western Area ATTN: MTW-IN
Oakland Army Base
Oakland, CA 94626-5000

Telephone No.

Commercial No: 415-466-3031 *
Autovon: 859-3031 *
HOTLINE No: 800-331-1822

California only: 800-348-4639

APPENDIX XVI. PERSONNEL SECURITY QUESTIONNAIRE (PSQ) ELECTRONIC TRANSMISSION PROGRAM

A. General. This appendix sets forth the procedures for the PSQ Electronic Transmission Program. This program enables the contractor to electronically transmit forms to DISCO and to receive forms and letters electronically from DISCO. This is a voluntary program open to all facilities.

B. Background.

1. The objectives of the PSQ Electronic Transmission Program are to:

a. Provide an automated means by which contractors can submit required forms to DIS and receive forms and correspondence electronically.

b. Reduce or eliminate the mail time between the contractor and DIS.

c. Significantly reduce the cost to contractors who must employ but cannot fully utilize employees awaiting security clearances.

d. Virtually eliminate the rejection of incomplete PSQ's through software edits and validations which ensure that forms contain complete and consistent information.

e. Provide the basis for future automation between DIS and contractors, among contractors, and within DIS.

f. Allow contractors to totally automate the security clearance internal processing and procedures and interface with existing data bases, e.g., personnel records, when completing security clearance applications and related paperwork, e.g., DISCO Form 562.

2. As program sponsor, DIS retains rights to all software designed to automate Department of Defense, Defense Investigative Service, and Defense Industrial Security Clearance Office forms. DIS will control the dissemination of this software to contractors and certify a contractor's eligibility to participate in this program.

3. The PSQ Electronic Transmission Program operates on a public data network provided by a vendor. The vendor is responsible for the development of the applications software for the network. The vendor is also responsible for the marketing and distribution of this software, development and distribution of user manuals, the provision of software updates based on DIS specifications, telecommunications services, and management of the network. The vendor provides 24 hour help-line assistance. All problems related to software use and telecommunications should be referred to the vendor.

4. The contractor must contact the vendor to participate in the PSQ program. The vendor will provide an information packet which contains an equipment survey, the computer services agreement and a pricing schedule. The vendor is:

CompuServe
Suite 920, Park Place
1655 North Fort Myer Drive
Arlington, VA 22209
Attn: Michael J. Mahoney
(703) 524-6900

5. All information will be encrypted utilizing a Data Encryption Standard (DES) Program before it is transmitted over the network. The contractor will have access only to information originated at the facility or transmitted to the facility's electronic mailbox from DISCO.

C. General Requirements. Basic requirements for participating in the PSQ electronic transmission program are as follows:

1. Costs. The contractor is responsible for all costs relating to the receipt of electronic data from the host computer maintained by the vendor, the transmission of data from the contractor to the host computer, and the procurement and maintenance of the necessary hardware. The contractor is also responsible for contacting the vendor to procure the software and telecommunications services and establishing a contractual agreement with the vendor. A standard computer services agreement will be made available to contractors by the vendor.

2. Form Eligibility. All DD Forms 48 are eligible for submission under the electronic transmission program with the exception of requests submitted in conjunction with OODEP clearances and requests which require UA endorsement. As additional forms are developed for electronic transmission, the vendor will distribute software updates and DIS will publish additional procedures as necessary.

3. Completion of Electronic Forms. The contractor may interface with existing data bases or information systems to fill in data fields and expedite the completion of forms. However, the contractor must interface with the software certified by DIS And provided by the vendor before transmitting forms to DIS. All information which is transmitted to DIS must satisfy the edits and validations built into the vendor-furnished software package.

4. DD Form 48 Certification and Retention.

a. Before transmission of the DD Form 48, the applicant must sign a printed copy of the form. This copy must be an exact representation of the information which is transmitted to DISCO.

b. The contractor must retain the original signed copy of the printed DD Form 48 until clearance processing is complete, i.e., the LOC is received or the clearance is denied. This signed copy shall be released to DIS upon request.

c. When an applicant is terminated while the clearance is in process, the contractor must retain the original signed copy of the printed PSQ for one year subsequent to the date of termination.

d. The contractor should retain a data file copy of the DD Form 48 on the PC until the clearance processing is complete.

5. Transmission Schedule.

a. DISCO will communicate with the vendor twice daily, at 8:00 a.m. EST to download forms from their mailbox and at 4:00 p.m. EST to upload forms.

b. Contractors may place forms into the DISCO mailbox at any time; however, they will not be picked up by DISCO until 8:00 a.m. EST. Contractors are strongly urged to communicate with the vendor once daily to ensure the timely receipt of LOC's.

c. In the event that communications with the vendor are interrupted for an extended period of time, the contractor may mail the request packet, to include the PC generated PSQ and the FD 258, Fingerprint Card, to DISCO.

6. Fingerprint Card Processing.

a. The FD 258, Fingerprint Card will be mailed to the following address:

Personnel Investigations Center
Fingerprint Card Processing Center
P.O. Box 1083
Baltimore, MD 21203-1083

b. The Fingerprint Card must be mailed immediately after the DD Form 48 has been transmitted to the vendor.

c. Clearance processing will begin immediately upon receipt of the DD Form 48. The Fingerprint Card will be processed upon receipt. If DIS has not received the Fingerprint Card 10 days after receipt of the PSQ, notification will be transmitted to the contractor. The contractor will then have 20 days after the date of notification to resubmit the Fingerprint Card to the above address. If no Fingerprint Card has been received 30 days after the original PSQ submission date, clearance processing will be cancelled and the contractor will be notified.

d. To reinitiate an investigation cancelled due to non-receipt of the Fingerprint Card, mail the Fingerprint Card, a printed copy of the DD Form 48, and a copy of the electronic letter received from DISCO to:

Defense Industrial Security Clearance Office
Attn: S0850
P.O. Box 2499
Columbus, Ohio 43216-5006

7. Verification. The contractor will receive an electronic verification of receipt for each PSQ transmitted to DISCO. This verification should be received two days subsequent to the transmission. If verification is not

received, the contractor should retransmit the form. If verification for this second transmission is not received, the contractor should contact the vendor for resolution.

8. Letters of Consent. Contractors who participate in the electronic transmission program will receive all LOC's electronically. LOC's received electronically may be printed on paper in use at the receiving PC. The format will replicate the format on the DISCO Form 560 but will contain no signature block for the Director, DISCO. This printed information will serve as the LOC and should be handled in the same manner as the printed DISCO Form 560.

9. PSQ Reject Letters. In the event that an electronically transmitted DD Form 48 must be rejected by DISCO, the PSQ Reject Letter will be transmitted electronically to the contractor. After the corrections are made, the corrected DD Form 48 should be electronically transmitted to DISCO.

10. Standard Practice Procedures (SPP). The contractor is responsible for establishing and enforcing appropriate security measures to safeguard the data maintained on the PSQ System and ensuring that only authorized requests are submitted via this network. These procedures shall be included in the facility's SPP.

APPENDIX XVII. TRANSPORTATION PLAN/TRANSMISSION INSTRUCTIONS

The provisions of paragraph 5an require that transmission instructions or a separate transportation plan be included with any contract, agreement or other arrangement involving the release of classified material to foreign entities. The transportation plan or transmission instructions are to be submitted to and approved by DoD authorities. As a minimum either shall include the following provisions:

a. A description of the classified material together with a brief narrative as to where and under what circumstances transfer of custody will occur;

b. Identification, by name or title, of the designated representative of the foreign recipient government or international organization who will receipt for and assume security responsibility for the U.S. classified material. (Person(s) so identified must be cleared for access to the level of the classified material to be shipped);

c. Identification and specific location of delivery points and any transfer points;

d. Identification of commercial carriers and freight forwarders or transportation agents who will be involved in the shipping process, the extent of their involvement, and their security clearance status;

e. Identification of any storage or processing facilities to be used and, relative thereto, certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped;

f. When applicable, the identification, by name or title, of couriers and escorts to be used and details as to their responsibilities and security clearance status;

g. Description of shipping methods to be used as authorized by the provisions of paragraph 17, together with the identification of carriers (foreign and domestic);

h. When it is anticipated that the U.S. classified material or parts thereof may be returned to the United States for repair, service, modification, or other reasons, the plan or instructions must require that shipment shall be via a carrier of U.S. or recipient government registry, handled only by authorized personnel, and that the applicable Military Department (for foreign military sales (FMS)) or DIS (for commercial sales) will be given advance notification of the estimated time and place of arrival and will be consulted concerning inland shipment;

i. The plan or instructions shall require the recipient government or international organization to examine shipping documents upon receipt of the classified material in its own territory and advise the responsible Military Department in the case of FMS, or DIS in the case of commercial sales, if the material has been transferred enroute to any carrier not authorized by the transportation plan/instructions; and

j. The recipient government or international organization also will be required to inform the responsible Military Department or DIS promptly and fully of any known or suspected compromise of U.S. classified material while such material is in its custody or under its cognizance during shipment. *

APPENDIX XVIII. SPECIAL CONSIDERATIONS FOR STU-III TYPE I SECURE TELEPHONE UNITS AT CONTRACTOR FACILITIES

A. General. This appendix sets forth guidelines for use of third generation or "user friendly" Secure Telephone Units, i.e., STU-III's, when used to transmit classified information. Basic requirements and procedures for safeguarding classified information using this technology are set forth in existing ISM provisions. In that the intent of our national security policy is to facilitate the availability and use of STU-III's, few additional security requirements are being imposed. The provisions of this appendix have been developed to conform with and complement the National Security Agency's (NSA's) "Operational Doctrine for the STU-III Type I Terminal" which promulgates security requirements for operation and control of the terminal unit and its encryption keys. NSA's Controlled Cryptographic Item (CCI) agreement requires contractors to adhere to doctrine requirements for the operation and protection of CCI equipment. Specific requirements and procedures for the protection of COMSEC information are set forth in the DoD 5220.22-S, "COMSEC Supplement to the Industrial Security Manual" (CSISM).

B. Background.

1. The recent proliferation of new communications technology, while improving the overall quality and efficiency of our communications systems, has also made these systems vulnerable to unauthorized exploitation. Recognizing this vulnerability has helped to increase security consciousness and has emphasized the need to protect our classified communications.

2. In the past, an insufficient amount of equipment was available to secure our communications. In part, this was due to the high unit cost of existing equipment. In 1984, the NSA initiated an accelerated program to develop and field a new generation of secure telephones, the STU-III family of equipment. This was to help counter the exploitation of our communications systems by hostile intelligence services and other unauthorized persons. The overall objectives of the STU-III program were to develop a low cost, user-friendly security telephone that would be: the size of a conventional telephone; producible in volume quantities; available to a wide range of users; and compatible with existing communications systems. That goal has now been achieved.

3. Understanding the rationale for the policy approach set forth in this appendix is essential to ensuring a sensible and pragmatic introduction of STU-III's into contractor operations. The approach taken deals realistically with the most severe existing threat to the security of classified information - our telecommunications habits and practices - and makes maximum use of NSA's new STU-III technology. The bottom line is that substantial amounts of classified and sensitive unclassified information are leaking to our adversaries over nonsecure telecommunications circuits. As noted above, the STU-III provides a low-cost, user-friendly system to "button up" U.S. communications. National policy is to encourage the widespread implementation and use of the STU-III. Accordingly, the

guidance contained in this appendix has been designed to facilitate widespread use. In comparison, the alternative risks to classified information that may be created by permitting some residential installations, for example, are small indeed. The COMSEC revolution has arrived. It requires rebalancing our traditional perception of threats and vulnerabilities to make the most beneficial use of this new technology.

C. Types and Models of Equipment. Two types of STU-III telephone instruments (i.e., terminals), are being produced:

1. Type I: These terminals are Controlled Cryptographic Items (CCI). Type I STU-III terminals may be used to secure classified information, or unclassified but sensitive, voice or data communications when keyed with an appropriate level of keying material. STU-III terminals are considered keyed when keying material has been loaded and an authorized Crypto Ignition Key (CIK) is inserted. When keyed, they must be safeguarded to the same classification level that the keying material being used is authorized to protect. When unkeyed, they are considered high-value property and are to be protected as CCI in accordance with section XI of the CSISM. They are interoperable with Type II terminals at the unclassified level.

2. Type II: These terminals may only be used with unclassified keying material. Use of these terminals does not fall within the scope of this manual.

3. The STU-III family of equipment consists of a number of different models of telephone terminals.

a. The STU-III Low-Cost Terminal, currently being produced by four vendors, is a replacement for the standard office telephone. Available in single-line or five-button models, it functions in both secure and non-secure modes and may be ordered with many modern telephone features, such as last number redial, repertory dialing, colors, etc.

b. In addition to the Low-Cost Terminal, the STU-III will also be manufactured in Cellular, Mobile/Portable and STU-II compatible models. The STU-III Cellular Terminal will provide secure voice/data capability to the mobile radio-telephone environment using the standard commercial cellular radio system employed in the U.S. They are interoperable with all other STU-III's. The STU-III Mobile/Portable Terminal is a more rugged model made specifically for military field use and similar applications. The STU-IIIA is a modified terminal which is also compatible with the STU-II telephone and is intended for U.S. applications in the NATO environment, where the STU-II is the standard secure telephone. Other STU-III configurations are under development and may become available in the future.

D. General Requirements. Basic security procedures for transmitting classified information via the STU-III Type I terminal when keyed with classified keying material are as follows:

1. Standard Practice Procedures (SPP). The facility SPP must include security instructions which describe the controls necessary to protect classified information before, during and after transmission.

2. Security Education. Cleared employees must be educated in the required security procedures prior to using the STU-III in the secure mode. The FSO, COMSEC Custodian, Alternate Custodian and the User Representative must be COMSEC briefed. The User Representative may be COMSEC briefed by the FSO or either custodian. STU-III users (personnel who insert crypto ignition keys for the purpose of transmitting classified information) who do not have or require further access to COMSEC information or material as defined in paragraph 10a, CSISM, need not be COMSEC briefed. For such users of STU-III terminals, the education requirements described here shall replace the COMSEC briefing requirements in paragraph 10a, CSISM. All STU-III users must be educated, as a minimum, in: i) the need for sound security practices in protecting information transmitted over the STU-III; ii) the specific security requirements associated with the STU-III; iii) the security reporting procedures in the event of STU-III terminal malfunction or COMSEC incidents, and iv) what constitutes an unauthorized action with regard to STU-III utilization. This education shall be provided by the FSO, COMSEC custodian or a designated individual fully knowledgeable of STU-III procedures. Users shall be reeducated as required. Individuals who will use STU-III terminals only in the non-secure (unkeyed) mode do not need to be educated in STU-III security procedures.

3. Clearance and Need to Know.

a. All STU-III terminals are interoperable with one another in the secure mode. However, during secure calls the character display on each STU-III terminal will show only the highest clearance level common to both terminals. Therefore users must limit the clearance level of information transmitted during the call to that indicated in the display.

b. The terminal will also display some identifying information about the person/organization at the distant terminal. The persons using the STU-III terminals are responsible for verifying the clearance and need-to-know of the individual on the distant terminal. Personal/voice recognition or contractual relationships may be used for additional identification and need-to-know verification, as appropriate.

4. Safeguards During Use. A STU-III terminal is considered keyed when keying material has been loaded and an authorized Crypto Ignition Key (CIK) is inserted. When keyed, the terminal must be kept under the constant surveillance of an appropriately cleared person who is in a physical position to exercise direct security control over the unit, unless it has been installed in an approved restricted or closed area, or is otherwise safeguarded commensurate with the level of classified operations. Constant surveillance includes preventing unauthorized personnel from overhearing classified conversations or seeing classified materials if visual access is a factor.

5. STU-III Terminal Installation

a. Within Cleared Facilities. STU-III terminals in cleared facilities shall be installed only in private offices or work areas where access to the STU-III may be controlled in keeping with the requirements to protect CCI equipment. Terminals to be keyed at a classification level higher than the approved safeguarding capability of the facility shall be installed as described in paragraph 5b, below.

b. Outside Cleared Facilities.

(1) STU-III terminals keyed for classified use may be installed or utilized outside cleared facilities as indicated below only with the prior written approval of the FSO. The FSO will obtain a justification statement. A record of each approval shall be recorded and maintained by the FSO for two years from the conclusion of such installation or use. Such terminals may be installed only in areas and under conditions where access to the STU-III may be controlled in keeping with the requirements to protect CCI equipment.

(2) ISM paragraph 14e prohibits the removal of classified material to an employee's residence for "after-hours" work as a convenience. The purpose of this prohibition is to preclude inadvertent compromise of classified material due to its presence in an uncontrolled environment. Approval to install a STU-III terminal in a residence or personal vehicle does not rescind this prohibition. Affected employees shall be specifically educated on the unique hazards of these environments, to include the points indicated in (3) and (4) below, as appropriate.

(3) Special provisions must be included in the facility SPP which emphasize the fact that such uncleared locations are not authorized to possess or safeguard classified material. Procedures must be described and implemented to ensure that no classified material is introduced into these locations. In addition, should classified material inadvertently be produced as a result of a secure telephone conversation in such places, the emergency steps to be taken to immediately secure and safeguard that material must be outlined in the SPP. AIS systems and facsimile machines shall not be connected to STU-III terminals installed outside cleared facilities.

(4) The CCI portion of the STU-III Cellular Type I terminal is normally installed in the trunk of the vehicle. When unattended, vehicles so equipped shall be locked and the CIK, terminal mounting mechanism key and vehicle locking keys shall be removed. When STU-III equipped vehicles are turned over to maintenance personnel for service or repair, the CCI portion of the terminal shall be removed and appropriately safeguarded.

(5) STU-III terminals installed outside the U.S. may only be located within a U.S. controlled facility which is defined as a base or building, access to which is physically controlled by authorized U.S. government or U. S. government contractor personnel. All installations of STU-III terminals outside the U.S. shall be approved and documented in the same manner as for terminals installed outside cleared facilities within the U.S., as previously described in this paragraph. In addition, a copy of such approvals, together with a copy of such changes to the

facility SPP as may be necessary, will be furnished to the OISI. SPP provisions will specifically describe procedures implemented to preclude access to the facility and terminal by unauthorized personnel.

6. Crypto Ignition Key (CIK) Protection.

a. Because CIK's enable operation of the STU-III terminal in the secure mode, they must be protected against loss and unauthorized access or use.

b. Master CIK's are those which may be used to create additional CIK's. Because of the potential to create unauthorized CIK's, master CIK's will be safeguarded in a manner commensurate with the highest classification level of the information that the master enables the STU-III to protect. The Two-Person Integrity (TPI)/No-Lone Zone (NLZ) controls described in section XI of the CSISM are not required for master CIK's that enable the STU-III terminal to transmit TOP SECRET information.

c. CIK's created for operational use, when not inserted in a STU-III terminal, will be kept in the immediate personal possession of an authorized user, or stored as indicated below.

1. If the CIK is to be stored in the same room as the STU-III terminal, it must be stored in a manner commensurate with the highest classification level of the information that the CIK enables the STU-III terminal to protect. As in 6b above, TPI/NLZ controls are not required to protect the CIK.

2. If the CIK is to be stored in a facility or location where a STU-III has been installed but in an area apart from the STU-III terminal, it must, as a minimum, be stored in a locked cabinet or desk, sufficient to reasonably preclude the ability of an unauthorized person to use the CIK in its associated STU-III terminal. Again, TPI/NLZ controls are not required to protect the CIK.

7. Use with Facsimile (FAX) Machines. Facsimile machines may be used to transmit classified information via the STU-III Type I terminal between and among cleared contractors with appropriate safeguarding, and UAs. FAX machines increase the difficulty of maintaining accountability and control of classified information. Therefore, users must be made aware of the vulnerabilities, and familiarize themselves with contractor procedures, specifically described in the facility SPP, that ensure the applicable document control requirements are followed. Such FAX machines must be safeguarded the same as the associated STU-III terminal during classified transmissions. Hard copy material receipts and acknowledgment of receipt back to the sender are not required for classified material transmitted by the STU-III Type terminals. All other requirements of this manual apply.

8. Classified Keying Material. Accounting procedures and requirements for safeguarding classified keying material are described in the CSISM.

9. Summary of other ISM Provisions. For user convenience, other pertinent ISM requirements are highlighted below:

a. All security violations must be reported pursuant to the requirements of paragraph 6 of the ISM. All COMSEC incidents (formerly called insecurities) must also be reported pursuant to the requirements of section XVI of the CSISM.

b. In accordance with paragraph 13j and k, ISM, TOP SECRET information may be transmitted outside the facility only with the prior written consent of the contracting officer. A record must be kept of all aural (and other) access to TOP SECRET information as required by paragraph 13a.

c. Classified notes taken during conversations on STU-III terminals must be safeguarded during use in accordance with the requirements of paragraph 16, marked according to paragraph 11c(15), entered into accountability per paragraph 12 and safeguarded when not in use in accordance with the requirements of paragraph 14.

d. Transmittal of classified information to subcontractors must be in accordance with the requirements of paragraph 59.

e. Transmittal of classified information between parent and subsidiary organizations must be in accordance with the requirements of paragraph 72.

f. Transmittal of classified information between an HOF and divisions of MFOs must be in accordance with the requirements of paragraph 73.

g. When a STU-III is used as a data transmission device for an approved AIS, it must be identified as teleprocessing equipment, as required by paragraph 112d(5), ISM, and the AIS SPP must be revised accordingly.

APPENDIX XIX. INDEX

Access, 3a, 13a, 13b & c, 20c(1), 31.3,

Accountability records, 12a
    For AIS storage media, 116a

ACDA:
    Access Limited, 31.3
    Classified information, 20c

Addressing mail and shipments, 17k

Administrative measures regarding security violations, 5aj

ADP System: (See "Automated Information System (AIS)")

Advance shipping notice, 17c(5)(d), 17d(3)(d)

Adverse clearance actions, 5e

Adverse information:
    Reporting of, 5af, 6b(1)

Agreement, long-term visits, 40

AIS Security, definition of, 3c

Alarm systems: (See "Intrusion Detection System")

Alien, 3d (see "Immigrant Alien," 3av)

Alternate storage locations:
    Containers, 15d
    General, 15a
    Records, 15c
    Security clearance requirements, 15b

APO mail channels, 17c(2), 17e(3)

Application software, definition of, 3d.1

Assistance and cooperation, 5aa

Atomic Energy RESTRICTED DATA (see "RESTRICTED DATA")

Authority, authorization for:
    Alternate storage, 15a
    Applying classification, 10d
    Classification guidance, subcontractors, 60b
    Clearance Limitations, 20a
    Controlled areas, 34c

  Defense Courier Service, 17b(3), 17e(5)
  Destruction, 19b
  Disclosure at meetings, 5q, 9e
  Electromechanical devices, 36c
  Intrusion Detection System, 35c
  Interim clearances, 26c
  Licensing agreements, 21b
  Methods of destruction, 19c
  Public releases, 5o
  Regrading of documents, 11d
  Releases:
    between subsidiaries, 72b
    intelligence information, 5c 3/,
    to foreign governments, 48a
  Removal of material to residences, 14e
  Reproduction, 18a
  Retention of classified material, 5l, 5m, 64
  Sales literature, publishing of, 5p
  Secure electrical transmissions, 17c(4), 17d(1)
  Subcontracts:
    from foreign contracts, 66
    involving TOP SECRET, 59a
    with foreign industry, 65
  Termination of accountability, 12h
  Transmitting:
    material outside U.S., 17e
    NATO material, 88c, 88d
    TOP SECRET material, 5x, 13i, 17b
  Use of special features of design on foreign contracts, 5h
  Visits:
    involving NATO information, 52
    involving RESTRICTED DATA, 42
    to contractors, 41
    to User Agency activities, 43, 44, 45

Authorized persons,
  Definition of, 3e

Automated Information System (AIS):
  AIS security, definition, 3c
  Applicability, 101
  Application software, definition, 3d.1
  Approval, 5b, 103b, 112
  Audit trails, 111
  Clearance of media and equipment, 115
  Computer facility, definition, 3u.2
  Computer hardware, definition, 3u.3
  Concurrent processing, 104.1
  Declassification of media and equipment, 116
  Definition of, 3b
  Downgrading, 114
  Firmware definition, 3am
  General requirements, 103

    Modes of operation, 104
    Objectives, 102
    Personnel security, 105
    Physical security, 106
    Protected area, 3bp, 106e(4)
    Protection of software and data, 108.1
    Remote terminal, definition, 3bv
    SPP, 103b, 112d
    Standard Practice Procedure, 103b, 112d
    Storage media controls, 108.1e
    Subcontracting controls, 110
    System Security Officer (SSO), 103c
        definition, 3cj.1
    System software, definition, 3ck
    Transmission controls, 109
    Upgrading, 113

Badges:
    Clearance, color coding, 8a, 20f
    Employees, 8a
    Reporting, 8c
    User Agency installations, 8d
    Visitors, 8b

Bank, use of for storage, 15

Bankruptcy, reporting of, 6a(4)(e)

Bid material:
    Destruction, 19a and b
    Disposition of, 51
    Publication and distribution of, 5p(2)
    Unsolicited, 10g

Briefcase Inspections (see "Perimeter Controls")

Briefings (see "Security briefings")

Candidate Material, definition of, 3f

Carrier:
    Custodian, 3ac, App. IX
    Qualified, 3bs

Carve-out definition, 3f.1

Central station alarm system, 35a, 35(b)(2)

Certificates:
    Consultant, Type A, 68a
    Destruction, 19e
    Excluded parent, 72a
    NATO briefing, 85d
    NATO clearance, 55

  Representatives of foreign interest statement, 20k

Charts, marking, 11c(2)

Citizenship, proof of, 5ae, App. XII

Classification authority, 3g, 10d

Classification equivalents, foreign, App. XIV

Classification guidance:
  Biennial Review, 10b
  Dissemination outside, CONUS, 10h
  Distribution, required, 61
  For subcontracts, 60
  General, 10a
  Responsibilities, 5ad
  Retention, 10c
  Unsolicited bids, 10g
  When issued, 10b

Classified contracts:
  Definition of, 3i
  Reporting of unrelated material, 6a(18)

Classified information:
  Access to:
    ACDA, 24a(1)(d)
    By non-U.S. citizens, 31
    CNWDI, 118
    Defense Counsel in Criminal Cases, 3k, 11
    Definition of, 3j
    Emergency Higher Level Access, 20.1
    Limitations, 31.3
    Requirements for, 20
    TOP SECRET, 13
  Definition of, 3j
  Evidence of mail tampering, 6a(11), 7
    Loss, compromise, or suspected compromise, 7
  Hand-carrying aboard commercial passenger aircraft, App. X
  Unauthorized introduction into or from a cleared facility
    (See "Perimeter Controls")

Classified waste, 19f, 80c

Clearance (facility):
  Additional Personnel, 24
  Advertising, 20f
  Associations, 22a
  Certificate, foreign interests, 21a, App. I (para. L)
  Colleges and Universities, 22d
  Consultants, Type B, 69
  Corporations, 22a

    Definition, 3a1
    Exclusion procedures, 22e
    Executive committees, 22a(2), 22c(3), 22d(3)(b)
    FOCI, 21c,
    Freight Forwarders, 22g
    Licensing, patent, and trade secret agreements, 21b
    Multiple facility, 73
    Negotiators, 23
    Non-profit organizations, 22a
    OODEPS, 6a(4)(c), 22a(4), 22b(4), 22c(5), 22d(5)
    Parent-subsidiary, 72
    Partnerships, 22c
    Personnel clearances required in connection with, 22
    Processing Procedures, 21a
    Reciprocal, 31.3
    Records, 20i
    Representatives of a foreign interest, 22f, 6a(4)d
    Sole proprietorships, 22b
    Security agreement, 21a
    Temporary help suppliers, 74
    Termination of, 5n
    Verification of, 38a, 58a

Clearance (individuals):
    Access, 3a, 20c, 31
    Access limitations, 20c(1)(2)(3)(4), 31.3,
    Additional personnel, 24
    Administrative downgrading of TOP SECRET and SECRET, 30
    Administrative termination, 29
    Adverse clearance actions, 5e
    Advertising, 20f
    Age limitations, 20b
    Application for, 26, App. XVI
    Assurance, security:
      application for, 99a
      issuance of, 99a
      termination of, 99a(5)
    Concurrent, 26f
    Contractor clearances, 24b
    Conversion of:
       Department of Energy, 27d
       Military Personnel, 27b
       National Guard or Ready Reserve Program 27c
       U.S. Government personnel, 27a
    DoD clearance, 24a
    DOE, 27d
    Downgrading, 30
    Electronic transmission of clearance application, App. XVI
    Emergency higher level access, 20.1
    Foreign nationals, 31, 31.2, 31.3
    Formerly cleared, 26d
    Full investigative coverage, 20g
    General information, 20, 26a

Granted by:
  contractor, 24b
  DoD, 24a
Guards, 20e
Immigrant aliens, 26b(2)(d), 31.1, 31.3
Interim clearances, 26c
Leave of absence from employment, 20h
Letter of Consent:
  definition of, 3az.1
  issuance of, 20j, 26h(1)(2)
  overseas assignment, 96
  reproduction of, 20f, 26h(1)(c)
Limited Access Authorizations for:
  immigrant aliens, 31.1, 31.3
  foreign nationals, 31.2, 31.3
Multiple facility, 20d, 20j, 26e
Name change, 6b(2), 26h(1)(e)
Negotiators, 23
New clearances, 26b
Non-United States citizens, 31
Preemployment clearance action prohibited, 25
Records, 28
Reemployment, of cleared personnel, 26d
Reinstatement, 30b
Representatives of foreign interest, 3bw, 20k, 22f
Required for:
  colleges and universities, 22d
  corporations, 22a
  partnerships, 22c
  sole proprietorships, 22b
Transfers, 26d, 26e
Withdrawal, interim clearances, 20m

Closed areas, 3m (also see "Controlled areas")

Closed vehicle, 3n

Cognizant security office, 3p, 4

Colleges and Universities, 3q

Combinations:
  Access to, 14c
  Changing, schedule for, 5i
  Classifying, 5i
  Door devices, 36b
  Knowledge of, 14c
  Padlocks, security, 5i
  Personnel authorized to change, 5i
  Security enclosures, 36a(1)

Commercial Carrier, 17c(5), 17d(3)

Communications Intelligence, 3r

COMMUNICATIONS SECURITY (COMSEC):
  Access limited, 20c(1)(2)(3), 31.3
  Briefing and debriefing, 5g
  Clearances, 24a(1)(a),
  COMSEC supplement, 76
  Definition, 3s
  Destruction, 19b
  Transmission, 17j
  Violations:
    investigation of, 7d
    reporting, 6a(3)

Complex, definition of, 3t

Compromise or suspected compromise:
  Definition, 3u
  Investigation of, 7
  Reporting, 6a(2)

Computer Facility, definition of, 3u.2

Computer tapes, magnetic:
  Declassification, 116a, 116b, 116c(3), 116c(4),
  Marking, 11c(11)

CONFIDENTIAL material:
  Clearances for access to, 24b,
  Definition, 3v
  Destroying, 19d
  Preparation for transmission, 17a
  Receipts, 12e(2)
  Records, 12c
  Release or transmission outside contractor's facility, 5x
  Storage, 14a(5)
  Supplemental controls, 14a(5)
  Transmission outside a facility, 5x, 17d,
  Transmission within a facility, 17a(3)

Consignee, 3w

Consignor, 3x

Constant Surveillance Service (CSS), 3x.1, 3cg, 3cm.1, 17d(3)(b)

Consultants:
  Access to CNWDI, 122
  Letter agreement, 70a, App. I(V)
  Temporary help suppliers, 74f
  Type A, 68
  Type B, 69
  Type C, 70
  Under civil service procedures, 71

Containers (see "Storage")

Continued classification after public release, 10i

Continental United States, definition of, 3y

Contract Security Classification Specification, 10a, 10b, 60, 61, App. I(G)

Contracting officer, 3z

Contractor, definition of, 3aa

Contractor-granted clearances, 24b:
- Administrative Termination of, 29a, 29c, 29d
- Reinstatements, 29h

Control station personnel, 12d

Control station records:
- Accountability, 12a
- Destruction, 19e
- Inventory lists, 17i
- Production, 12f
- Production control, 78
- Receipts, 12g
- Receipts and dispatch, 12c
- Reproduction, 18c

Controlled areas, 5r:
- AIS protected area, 3bp, 106d(4)
- Approval for, 34c
- AIS system area controls, 106
- Basis for, 33
- Closed areas:
  - construction, 34a, App. V
  - definition, 3m
  - identifying, 34a(4)
  - nonworking hours, 34a(3)
  - working hours, 34a(2)
- Reports, 6a(5), 34d
- Restricted areas:
  - definition, 3bx
  - marking, 34b(3)
  - nonworking hours, 34b(2)
  - working hours, 34b(1)
- Supplemental or supplanting controls (see "Intrusion Detection System")

Cooperation, 5aa

Courier, 17c(3), App. X

Cover sheets, 11b(2), 11c(5)

Covering:
  - Documents in use, 16b
  - Equipment, 17a(1)(c)

Credentials:
  - Recovery of, 8a(5)
  - Verifying, 8a(6)

Critical Nuclear Weapons Design Information (CNWDI):
  - Access requirement, 118
  - Briefings, 119
  - Definition, 3o
  - Marking, 121
  - Policy, 117
  - Records, 120
  - Subcontracting and consultants, 122
  - Transmission outside facility, 123

CRYPTOGRAPHIC (CRYPTO):
  - Accounting for, 12a
  - Definition, 3ab
  - Inventory and accounting, 12b
  - Production of, 12f(1)
  - Reproduction, 18a, 18c

Dates, required on classified material, 11b(1), 11c(15)

Declassification, definition of, 3ad, App. II

Defense Courier Service, 17b(3), 17e(5)

Degaussing, 116b

Delay in shipment, 6a(10), 17c(5)(d), 17d(3)(d)

DoD technical information dissemination activities, 5y

Design features, incorporation of, 5h

Designated countries, 3ag.1

Designated country relationships, 5v, 6b(4)

Designated country visits, 6a(19)

Destruction:
  - Authorization, 19b
  - Certificates, request for, 19e
  - Classified waste, 19f
  - Destroying official, 19d
  - Equipment approval, 19c
  - Inspection of equipment, 19c(8)
  - Methods, 19c

  Records and certificates, 19e
  Rented or leased equipment, 19c
  Reproduction materials, 80, 81
  Requirement of, 19a
  Ribbons, typewriter and ADP, 19f
  Subcontractor employee, use of, 19d
  Witness, 19d

Determining need-to-know, 5f

Disclosures:
  At meetings, 5q, 9e
  Limitations on, 5c
  Public, 5o
  To subcontractors, 58a, 59

Disk and drum, declassifying, 116c(6)

Dispatch records, 12g

Disposition of classified material, 51

Documents:
  Definition of, 3ah
  Letters of transmittal, 11c(13)
  Marking of, 11

Downgrade:
  Clearances, 30
  Definition, 3ai, App. II:

Electrical transmission, 17b(2), 17c(4), 17d(1), 109, App. XVIII

Electromechanical devices:
  Approval, 36c
  Door devices, 36a
  Security enclosures, 36a(1)
  Supplemental, 36b

Electronic devices:
  Approval, 36c
  Door devices, 36a(2)
  Security enclosures, 36a(1)

Emergency Higher Level Access, 20.1

Emergency procedures, 5w

Employee badges, 8a

Energy Department (DOE) facilities, visits to, 46

Escorts:
  For AIS maintenance, 105d
  For transmission, 17c(3), App. IX
  For visitors, 38b

Espionage and Sabotage Acts, App. VI

Evidence of tampered mail, 6a(11), 7 16/

Exclusion of personnel:
  From clearance requirement, 22e

Executive committee, 22a(2), 22c(3), 22d(3)(b)

Executive personnel, 3aj

Export Licenses:
  Unclassified technical data, 41d

Facility, 3ak

Facility security clearance, al, (see "Clearance")

Facility security supervisor, 5a

FBI, reporting to, 7b(1)

File folders, marking of, 11c(5)

Files, classified, 11c(5)

Fingerprints, 26a(3), 26a(4),

Firmware, definition of, 3am

Foreign:
  Classification equivalents, App. XIV
  Classified contracts, App. III
  Government information, definition of, 3an
  Interest, 3ao
  Licensing, Patent, and Trade Secret Agreements, 21b
  Marking foreign classified material, 11e, 11b(5)(a), 11b(8)(e), 11b(8)(f)
  Nationals, 3ap, 31.2, 31.3
  Ownership, control, and influence, 21c, 72a, App. I(M)
  Representatives of foreign interest, 3bw
  Travel, 5u, 6b(9)

FORMERLY RESTRICTED DATA:
  Access limited, 20c(1), 20c(2), 20c(3), 31.3
  Definition, 3aq
  Dissemination, 171
  Marking, 11b(8)(b)

Freight Forwarder, 17o

General requirements, 5

Graphic arts, definition of, 3ar (also see "Reproduction")

Groups of documents, 11c(5)

Guards:
    Clearance of, 20e
    Emergencies, use of, 5w(1)
    Entry Control:
        closed areas, 34a(2)
        facility complex, 14a(4)(a)
        meetings, 9d(4)
        room, building, structure, 14a(2)(a), 14a(4)(a)
        safe deposits area, 15b
    Patrols:
        of closed areas, 34a(3)
        of room, building, structure, 14a(2)(b), 14a(4)(b)
        of strongrooms, 14a(3)(f)
    Response to alarms, 35a(1), 35a(2)
    Subcontract:
        Destruction of CONFIDENTIAL waste, 19f
        Witness to destruction, 19d

Guidance for contractor self-inspections, App. XIII

Guides, classification, 10a, 58

Hand-Carrying Classified Material Aboard Commercial Passenger Aircraft, App. X

Hardened container, 3as, 17a(2)(a)

Hardware, Computer, definition of, 3u.3

Home office (HOF), 3at

Immigrant alien:
    Access Limitations, 31.3
    Clearance of, 31.1
    Definition of, 3au
    Justification and approval for clearance, 31.1
    Limitations, 118
    Reinstatement of LAAs, 31.1e
    Termination of LAA, 29
    Visiting overseas, 6b(6)

Identifying facility of origin, 11b(1)

Individual responsibility for safeguarding, 5f

Industrial security, 3av

Information, definition of, 3aw

Inspections, 5ac, 5ag. App. XIII

Intelligence, 3az

Intrusion Detection System:
- Approval, 35c
- Central control station, requirements for 35a(1)
- Direct connect, 35a(1)(a)(b), App. XI
- Material and installation, standards for, 35b, App. XI
- Purpose, 35a
- Records, 35a(1)(h)
- Response time, 35a(1)(f), 35a(2)
- Supplanting, 35a(1), 36a
- Supplemental, 14a(2)(c), 14a(4)(c), 35a(2), 36b

"International Traffic in Arms Regulation", 21b, 41d, 48a(3), 48b, 50, App. VII

Interpretations, requests for, 4

Inventory, in connection with visits, 17i

Inventory and accounting of classified material, 12b

Investigations:
- By contractors, 7
- By U.S. Government representatives, 5aa

Investigative assistance, 5aa

Justification for Personnel Security Clearance:
- Additional LOCs, 26(h)(2)(b)
- Clearance conversions, 27
- Clearance transfers, 26d
  - MFO: 26e
- Concurrent clearances, 26f(1)
- Contractor granted, 24b
- DOE and NRC clearances, 27d
  - Example of form, App.I, para. I
- New clearances, 26b
- Reemployment, 26d
- Reinstatement, 29g, 29h, 29i, 30b
- Requirements:
  - management review, 20a
  - completion of forms, 26a
- Retention, 20a
- Termination: 29
  - subsequent access, 29g, 29h

Legends, markings, 11c(2)

Letter of Consent (LOC), 3az.1, 20f, 20h, 20j, 20.1, 22a(4), 22c(5), 26d, 26e, 26f, 26h,

Limitations on:
    Access to classified information, 20c, 24b, 31.3
    Destruction, 19b
    PCL's, 20a
    Reproduction, 18a, 87a

Limited Access Authorization (LAA)
    Definition, 3az.2
    Immigrant Alien processing, 31.1
    Foreign national processing, 31.2

Limited Dissemination (LIMDIS)
    Definition, 3az.3
    Security cognizance of, 5ao

List of Classified Contracts, 5ag

List of OODEPs, 6a(4)(c), 22a(4), 22b(4), 22c(5), 22d(5)

Location of meetings, 9c

Locked Entrance:
    Closed areas, 34a(2)(b), 34a(3)
    Definition, 3ba
    Room, building, structure, 14a(2)(a), 14a(4)(a)

Long-term visitors, 40

Machine accounting cards, marking of, 11c(3)

Machine listings, marking of, 11c(4)

Magnetic tapes, degaussing, 116b, 116c(3), 116c(4)

Maps, marking of, 11c(2)

Markings:
    Artwork, 11c(1)
    AIS produced document, 11c(4)
    ADP punched cards, 11c(3)
    Automatic downgrading or declassification actions, 11d(1)
    Blankets, 80f(2)
    Charts, 11c(2)
    Compilations, 11g
    Components, 11b(4)
    Containers (transmission), 17a(1), 17a(1)(e), 17a(2)(a)
    CNWDI, 12i
    DTIC documents, 11d 3/
    Dissemination and reproduction notices, 11b(8)(d)
    Downgrading and declassification, "Classified by" notice, 11b(7), App. II (B2)
    Drawings, 11c(2)
    Files, folders, or groups of documents, 11c(5)
    Foreign classified material, 11b(5)(a), 11b(8)(e), 11e

- Foreign government information, 11b(8)(e)
- FORMERLY RESTRICTED DATA notation, 11b(8)(b), App. II
- General, 11a
- Identification, 11b(1)
- Intelligence sources or methods of notation, 11b(8)(c)
- Linecasting machines, 79b
- Maps, 11c(2)
- Messages, 11c(6), App. II
- Microforms, 11c(7)
- Miscellaneous material, 11c(16)
- Motion picture films, 11c(8)
- NATO extracts, 11b(8)(f)
- Origination date, 11b(1),
- Other than automatic downgrading or declassification action, 11d(2)
- Overall, 11b(2)
- Overlays, 11c(1)
- Pages, 11b(3)
- Photocomposition machines, 79b
- Photographs, 11c(9)
- Plates, reproduction, 80f(3)
- Portions, 11b(5)
- Presses, reproduction, 79a
- Production control records, 78
- Punched cards, 11c(3)
- Recordings (sound, magnetic, electronic, and other), 11c(10)
- Regraded documents and material, 11d
- Removable ADP and word processing storage media, 11c(11)
- RESTRICTED DATA notation, 11b(8)(a), App. II
- Rolled or folded documents, 11c(2)
- Subjects and titles, 11b(6)
- Tentative, 10g(2)
- Titles, 11b(6)
- Tracings, 11c(2)
- Translations, 11c(12)
- Transmittals, 11c(13)
- Transparencies and slides, 11c(14)
- Upgrading, 11d(3)
- Wholly unclassified material, 11f
- Working papers, 11c(15)

Material, 3bb

Mechanical Devices:
- Approval, 36c
- Door Devices, 36a(2)
- Security enclosures, 36a(1)

Meetings:
- Disclosure at:
  - Contractor facilities, 5q(1), 5q(3)
  - DoD, 5q(2)
  - Other User Agencies, 5q(4)

    DoD sponsorship:
      attendance of foreign nationals or representatives of a foreign interest, 9b
      location, 9c
      requests for, 9a
      requests for disclosure authority, 9e
      requests to attend, 9f
      security procedures, 9d

Multiple facility organizations:
    Classification guidance, 73c
    Clearance records, 28
    Collocated facilities, 72c
    Concurrent clearances, 20j, 26f
    Definition of, 3bc
    Exchange of employee rosters, 37g
    Interchange of classified information, 72c, 73b
    Issuance of LOC's, 26h(2)
    Personnel clearances, 20d, 73d
    Principal Management Facility (PMF), 3bo
    Security clearance administration, 73e
    SPP, 5s(1), 72c, 73a
    Transfers, 26e
    Visits between, 72c, 73e(3)

National of U.S., 3bd

NATO classified information:
    Access record, 85b
    Authority, 84
    Briefing, 85c, 85d
    Certificate of security clearance, 55
    Clearances, 24a(1)(c), 86
    Combination, changing of, 51
    Contracting officer functions, 89
    Definition of, 3bf
    Disposition, 19b, 19c
    Marking, 87b
    Reporting receipt of, 90
    Reproduction, 87a
    Security supervisor, 85a
    Subcontracting, 91
    Transmission:
      outside U.S., 88c, 88d
      within U.S., 88b
    Visits involving, 52, 53
    Visit records, 54

Need-to-know, definition of, 3bg

Negotiator, definition of, 3bh

Notations:
    Dissemination and reproduction, 11b(8)(d)
    Downgrading or declassification, 11b(7), App. II
    Foreign government information, 11b(8)(e), 11e
    FORMERLY RESTRICTED DATA, 11b(8)(b), App. II
    Intelligence sources and methods, 11b(8)(c)
    NATO information, 11b(8)(f)
    RESTRICTED DATA, 11b(8)(a), App. II

Notification of Postal Authorities, 6a(11), 7

Nuclear Weapon Security Program, 3bi, 20c,

Office of Industrial Security, International, 95

Officers, definition of, 3bj

Operations Security (OPSEC):
    Applicability, 126
    Contractor requirements, 5ai
    Definition, 3bk.1
    EEFI, 3ai.1
    General, 125
    Indicators, 3bk.2
    Purpose, 124
    Scope, 1h
    Self-inspecting procedures, 127

Orientation of personnel, 5f, 5g

Overseas operations,
    Access to U.S. classified information:
        general, 92, 93
        notification of overseas assignment, 96
        overseas assistance, 95
        rejustification of clearance requirement, 95
    Reporting requirements for foreign travel, 6b(9), 92d,
    Safeguarding U.S. classified information, 94
        custody and storage, 94c
        disclosure, 94d
        security classification guidance, 94a
        transmission, 94b
    Security briefings and certificates, 97
    Access to classified information of foreign governments and international pact organizations under a security assurance:
        general, 98
        security assurance, 99

Parent, definition of, 3bl.1

Parent-subsidiary:
    Clearance requirements, 72a
    Collocation of facilities, 72c

- Exclusion action, 72a
- Interchange of classified information, 72b

Patentable material, 5m(1)(b)

Patrols, patrolling:
- Closed areas, 34a(3)
- Facility complex, 14a(4)(b)
- Rooms, buildings, structures, 14a(2)(b), 14a(4)(b)
- Strongrooms, 14a(3)(f)

Perimeter controls, 5am

Personnel:
- Clearance (see "Clearance (individuals)")
- Exclusion, 5e
- Identification, 8
- Suspected compromise, investigation of, 7

Personnel Security Clearance (PCL), 3bm

Possessions, 3bn

Preemployment Clearance Application, 25

Principal management facility (PMF), 3bo, 73

Printing (see "reproduction")

Production of classified materials:
- Incorporation of, 12f(4)
- Other material, 12f(3)
- SECRET documents, 12f(2) TOP SECRET, CRYPTO, and special access documents, 12f(1)

Protected area, definition, 3bp

Protective Security Service, 3bq, 3cq, 3cm.1, 17a(2)(b), 17c(5)(b)

Public disclosure, 5o (also see "Disclosure")

Pulping (for destruction), 19c

Qualified carrier, 3bs, 17c(5)

Receipts:
- Inner containers, inclusion, 12g(2), 17a(1)
- Obtained during visits, 17i
- Retention of, 12g(3)
- Signing and return of, 12e(2)
- Suspense file and follow-up, 12g(3)
- Within a facility, 13d

Receipt and dispatch records, 12c
        Receipt of classified material, 12e

Record of:
    Accountability, 12a
    Alternate storage facilities, 15c
    Badges and identification cards, 8a(5)
    Citizenship, App. XII Clearances, 28
    Combinations, knowledge of, 14c
    Control cards, electronic, 36a(2)(a), 36b
    Control station personnel, 12d
    CNWDI, personnel having access to, 120
    Destruction, 19e
    Discussions and photographs, 38c
    Dispatch of classified material, 12g
    Inventory and accounting, 12b
    Inventory, visits, 17i
    NATO access, 85b
    NATO visits, 54
    Production control, 78
    Production of classified material, 12f
    Receipt and dispatch, 12c
    Receipt of classified material, 12e
    Reproduction, 18c
    Retention of, 5m
    Termination of accountability, 12h
    TOP SECRET access, 13a
    Visitors, 39

Reference material, 3bt

Registry, central, 87a, 90

Regrading:
    Authority, App. II
    Definition of, 3bu
    Marking, 11d

Release of classified information, 5x

Removal of classified material to residence, 14e

Reports, reporting:
    Adverse information, 6b(1)
    Assignment of immigrant aliens, 6b(6)
    Attendance at meetings, 5u(1), 6b(9)
    Authorization to apply classifications, 6a(14)
    Badges and identification cards, 6a(13)
    Category of classified information, 6a(8)
    Changed conditions, 6a(4)
    Change in closed or restricted area, 6a(5)
    Change in employee's status, 6b(2)
    Change in storage capability, 6a(6)

  - Citizenship by naturalization, 6b(7)
  - Delay in shipment, 6a(10)
  - Employee information in compromise cases, 6a(7)
  - Employees desiring not to perform on classified work, 6b(10)
  - Espionage, sabotage, or subversive activities, 6a(1), 6c
  - Evidence of tampering, 6a(11)
  - Foreign classified contracts, 6a(17)
  - Improper shipment, 6a(12)
  - Inability to safeguard classified material, 6a(16)
  - Location or disposition of classified material, terminated from accountability, 6a(15)
  - Loss, compromise, or suspected compromise, 6a(2), 7
  - Official investigation, 6b(3)
  - Other security violations, 6a(3)
  - Personal exchange with representatives or nationals of Designated countries, 6b(9)
  - Preliminary inquiry, 7d
  - Receipt of classified information not related to a classified contract, 6a(18)
  - Relationships in Designated countries, 5v, 6b(4)
  - Representative of a foreign interest, 6a(4)(d), 6b(5)
  - Termination of business, 6a(4)(e)
  - Travel or attendance at meetings, 5u(1), 6b(9)
  - Visits by Designated country representatives or nationals, 6a(19)

Representatives of a foreign interest, 3bw, 20k, 22f

Reproduction:
- Area controls:
  - bindery areas, 79c
  - composition areas, 79b
  - darkrooms, 79d
  - pressrooms, 79a
  - proofreading areas, 79e
  - shipping entrances, 79f
- Authorizations for, 18a
- Blankets, rubber, 80f(2)
- Blankets, other than rubber, 80f(3)
- Bulk shipments, 80e
- Designation of equipment, 18
- Destruction, special requirements, 81
- Identification of:
  - linecasting machines, 79b
  - photocomposition machines, 79b
  - presses, 79a
- Mailing lists:
  - classified, 82a
  - related material, 82c
  - unclassified, 82b
- Overruns, 80a
- Plates, 80f(3)
- Press, parts of, 80f(4)

- Production material, 80f(1)
- Proofs, 80b
- Records:
  - control stations, 18c
  - production control, 78
- Regraining of plates, 80f(3)
- Samples, return of, 80d
- Waste, disposal of, 80c

Restricted Area, bx (see "Controlled areas")

RESTRICTED DATA:
- Access limited, 31.3
- Clearance for access to, 24a(1)(a)
- Definition of, 3by
- Dissemination, 171
- Marking, 11b(8)(a), App. II
- Violations involving, 7d
- Visits involving, 42, 46, 47

Retention of classified material:
- By subcontractors, 64
- General, 5m, 10c

Return of classified material, 51, 64,

Return of samples, 80d

Safeguarding:
- General, 5d
- Individual responsibility, 5f
- Verification of, 59b

Safeguarding U.S. information overseas:
- Custody, 94c
- Disclosure, 94d
- Storage, 94c
- Transmissions, 94b

Safeguards during use, 16

Sales literature, 5p

SECRET material/information:
- Accounting for, 12a
- Authority for:
  - disclosure at meetings, 9e
  - removal to residence, 14e
  - reproduction, 18a
  - transmission, 17e
- Clearance for access to, 24a, 26c
- Definition, 3bz
- Destruction of, 19d, 19e

    Inventory and accounting, 12b
    Preparation for transmission, 17a
    Production of, 12f
    Receipts for, 12g, 17a
    Release or transmission outside contractor's facility, 5x
    Storage:
      containers, 14a(3)
      supplemental controls, 14a(4)
    Transmission:
      by commercial carrier, 17a(2)
      outside a facility, 17c
      outside U.S., 17e
      preparation for, 17a(1)
      within a facility, 17f

Secure Telephone Unit ("See STU III")

Security, agreement:
    Execution of, 21
    Termination of, 5n

Security briefings and debriefings:
    COMSEC, 5g
    CNWDI, 119
    Defensive, 5u, App. VII
    Destruction, official, 19d
    Individual responsibilities, 5f, App. VII
    NATO, 85c
    Overseas assignment, 96
    Refresher, 97c, 97d
    Security briefing and certificates, overseas, 97
    Security briefing and termination, 5g
    TOP SECRET, 5g, 13b
    Visitors, Category 5, 41e
    Visitor escorts, 38b

Security checks, 5j

Security cognizance, 1d, 3cc

Security, definition of, 3cb

Security education, 5f

Security enclosures, 36a(1)

Security inspections, 5ac, 5ag

Security of combinations, 5i

Security supervisor (see "Facility security supervisor"), 5a

Security violations, 5aj, 6b(1), 6a(3)

Self-inspection, 5ac

SENSITIVE COMPARTMENTED INFORMATION:
- Clearances, 24a(1)(a), 75d
- Contracts, 75b, 75c
- Definition of, 3cd

Shipments:
- Bulk, 80e
- Notification of consignee, 17c(5)(d)
- SECRET, controlled, 3ca

Shipper, 3ce

Short title, 3cf

Shredders, 19c

Signature and Tally Record, definition of, 3cg

Single line service, 3ch

Special access programs, 3ci, 5t

Special features of design, 5h

Sponsorship of Freight Forwarders, 21d

Standard Practice Procedures,
- AIS, 112d
- Collocated facilities, 72c
- Destruction procedures, 19c(4)
- Emergency procedures, 5w
- Limiting PCL's, 20a
- Security controls in multiple facility organizations, 73
- Security procedures of overseas locations, 97e

Standards, Underwriters' Laboratories, 35b

Storage:
- Alternate storage locations, 15
- Bulky material, 14b
- Classified waste, 19f
- CONFIDENTIAL material, 14a(5)
- Desk pedestals, 14a(3)(g)
- En route to destination, 17h
- GSA approved cabinets, 14a(1), 14a(3)(a)
- Lock bar, security of, 14a(3)(g)
- Overseas, 94c
- Private residence, 14e
- Protection during nonworking hours, 14d
- SECRET material, 14a(3), 14a(4)

  - Steel file cabinets, 14a(3)(d)
  - Supervision of containers, 14c
  - Supplemental controls for:
    - SECRET material, 14a(4)
    - TOP SECRET material, 14a(2)
  - TOP SECRET material, 14a(1)
  - Vaults:
    - Class A, 14a(1), App. IV
    - Class B, 14a(3)(b), App. IV
    - Class C, 14a(3)(e), App. IV

Strongrooms, 14a(3)(f), App. IV (para. F)

STU III, App. XVIII

Subcontractors, vendors and suppliers:
  - Approval of requests from, 56
  - Badging of, 8a(7)
  - Classification guidance, 60
  - Clearance status of, 58
  - CNWDI access, 122
  - Disclosure of TOP SECRET material to, 59a
  - Disposition of classified information, 64
  - Distribution of guidance, 61
  - NATO access, 91
  - Safeguarding ability of, 59
  - Selection, notification of, 62
  - Subcontracting on foreign contracts, 66
  - Subcontracting with foreign industry, 65
  - Telephone requests, regarding, 59b(4)
  - Unsatisfactory conditions at, 63
  - Visit requests for, 41a(3)

Subsidiary, 3cj

Supplanting IDS, 35a(1)

Supplemental IDS, 35a(2)

Symposium involving classified material, 5m(2)

System Security Officer (SSO), 3cj.1

System Software, 3ck

Temporary help suppliers, 5ab, 74

Tentative markings, 10g(2)

Termination of accountability, 12h

TOP SECRET:
- Access, general, 13b, 13g
- Access by employees working alone, 13c
- Access records, 13a
- Accounting for, 12a, 13f
- Authority for:
  - disclosure at meetings, 9e
  - disclosure to subcontractors, 59a, 13k
  - interim PCLs, 26c
  - removal to residence, 14e
  - reproduction, 13i, 18a,
  - transmission, 13j, 17b
- Clearance for access to, 26b(2)
- Control station personnel, 12d
- Definition of, 3cl
- Deliveries, 13g
- Destruction of, 19e
- Dissemination, 13d
- Inventory and accounting, 12b, 13f, 13h
- Preparation for transmission, 17a
- Production of, 12f
- Receipts for, 12g(2), 13e, 17a
- Release or transmission outside contractor's facility, 5x
- Reproduction, 13i
- Security assurance, issuance of, 99b
- Special requirements, 13
- Storage:
  - containers, 14a(1)
  - supplemental controls, 14a(2)
- Transmission:
  - method, 17b
  - preparation for, 17a(1)
  - within a facility, 17f
- Violation, involving, 7b

Transmission:
- Aboard aircraft, 17h, App. X
- Additional protection during visits, 17i
- Additional requirements, commercial carriers, 17a(2)
- Addressing mail or shipment, 17k
- Classified Material to Foreign Governments, 17m
- Commercial carrier, 17d(3)
- Definition of, 3cm
- Electrical, 17b(2), 17c(4), 17d(1), 109
- Inspection of classified mail and shipments, 12e(2),
- Method of transmitting:
  - COMSEC material, 17j
  - CONFIDENTIAL material outside facility, 17d
  - CNWDI, 123
  - NATO material, 38
  - outside U.S. and possessions, 17e, 94b
  - SECRET material outside of facility, 17c
  - SECRET and CONFIDENTIAL material within a facility, 17f

    TOP SECRET material outside facility, 17b
    TOP SECRET material within facility, 17f
  Notification of consignee, 17c(5)(d)
  Preparation for:
    CNWDI, 123
    outside a facility, 17a(1)
    within a facility, 17a(3)
  Protection en route, 17h Procedures for, 5k
  Report of evidence of tampering, 6a(11)
  Restriction for RESTRICTED DATA, 171

Transportation Plan/Transmission Instructions, 5an, Appendix XVII

Transportation Protection Service (TPS), 3cm.1

Transshipping, 3cn, 17c(5)(d)

Trust territory, definition of, 3co

Type A Consultants, 68

Type B Consultants, 69

Type C Consultants, 70, App. I(V)

Unauthorized persons, 3cp

United States, definition of, 3cq

Upgrade:
  clearances, 30b
  definition of, 3cr

User Agencies, 3cs

Vaults and strongrooms:
  Class A, 14a(1), App. IV
  Class B, 14a(3)(b), App. IV
  Class C, 14a(3)(e), App. IV

Verification of facility clearances, 38a, 58

Verification of facility safeguarding and storage, 59b(4)

Visitor badges, 8b

Visits:
  Advance notice, 37d
  Authority for, 37e(4)
  Carrying classified material on, 17e, 17f
  Category 1, 41a
  Category 2, 41b
  Category 3, 41c
  Category 4, 41d
  Category 5, 41e

  Control of, 38b
  Criteria for approval, 37b
  Disapproval notice, 37c
  Escorts, 38b
  Export license, 41d(3)
  Facility clearance, verification of, 38a
  Identification of visitor, 38a
  Industrial security representatives, 37h
  Involving RESTRICTED DATA, 42
  Long-term, 40
  Multiple facility organization, 73
  NATO visits:
    clearance certificate, 55
    definition of, 39b
    records of, 54
    recurring, 52d
  NPLO programs, 53
  Processing time, 49
  Recordings and discussion, 38c
  Records of, 39
  Recurring, 37f
  Removal of classified material, 38d
  Reporting Designated country visits, 6a(19)
  Requests, contents of, 37d, 41
  Telephone requests regarding, 37d
  Under bilateral agreements, 51
  Use of OISI for, 50

Visits to:
  DOE and its contractors, 46
  Foreign government and activities, 48
  Government activities other than DOE, 47
  User Agencies in the U.S., 44
  User Agencies outside the U.S., 45

Waste material, 19f, 80c

Weapon system, definition of, 3ct

Witnesses for destruction, 19d

Working hours, definition of, 14a(2)

Working papers, 11c(15), 12f

✿U.S. GOVERNMENT PRINTING OFFICE: 1989 234-655/00229